NOTE: IMPOUNDED MATERIAL IN THIS BRIEF HAS BEEN REDACTED

COMMONWEALTH OF MASSACHUSETTS

Supreme Judicial Court

SUFFOLK, SS. No. SJC-12946

ATTORNEY GENERAL,
Petitioner-Appellee,

v.

FACEBOOK, INC.,
Defendant-Appellant.

ON APPEAL FROM AN ORDER OF THE SUPERIOR COURT FOR SUFFOLK COUNTY

BRIEF FOR PETITIONER-APPELLEE ATTORNEY GENERAL MAURA HEALEY

MAURA HEALEY
Attorney General

Sara Cable, BBO # 667084
Jared Rinehimer, BBO # 684701
Assistant Attorneys General
Data Privacy and Security Division

Peter Downing, BBO # 675969
Assistant Attorney General
Consumer Protection Division

Public Protection & Advocacy Bureau
One Ashburton Place
Boston, Massachusetts 02108

sara.cable@mass.gov, (617) 963-2827
jared.rinehimer@mass.gov, (617) 963-2594
peter.downing@mass.gov, (617) 963-2014

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

STATEMENT OF THE ISSUES

In March 2018, the Attorney General opened a civil investigation into the potential misuse of consumers' personal data by developers of applications ("apps") used with Facebook's social media platform. The Attorney General later issued a Civil Investigative Demand ("CID") under G.L. c. 93A, § 6 requesting, among other things, (1) the identity of, and factual information about, apps and developers that may have misused consumer data, as identified in Facebook's App Developer Investigation ("ADI"), and (2) Facebook's internal communications about those apps and developers. In response, Facebook asserted that all the requested information was attorney work product and protected by the attorney-client privilege.

The questions presented are:

1. Whether Facebook failed to establish that information from its ADI was "prepared in anticipation of litigation," and thus work product, where Facebook widely publicized other purposes of the investigation and had, for the prior six years, undertaken similar investigations of app developers in the ordinary course of its business without asserting work product over those efforts.

2. Whether, in any case, the Attorney General is entitled to the factual information requested in the CID under Mass. R. Civ. P. 26(b)(3) because she has a

substantial need of the materials and is unable to obtain their substantial equivalent by other means, and disclosure will not reveal opinions or theories of counsel.

3. Whether Facebook failed to prove its blanket assertion of attorney-client privilege where (i) the CID sought facts developed in the ADI, not communications made in confidence to counsel, and (ii) to the extent the CID did seek internal Facebook communications, Facebook failed to submit a privilege log showing that each withheld communication met each element of the privilege.

4. Whether Facebook waived its objections to the CID because it failed to file a motion to modify or set aside the CID for good cause, as required by G.L. c. 93A, § 6(7).

STATEMENT OF THE CASE

This appeal stems from Facebook's refusal to disclose information in the Attorney General's investigation under G.L. c. 93A, § 6 into the potential misuse of consumers' personal data by developers of software apps that Facebook allowed on its social media platform. The Attorney General opened the investigation following public reports that one app developer had, several years earlier, taken personal data of 87 million Facebook users and sold it to Cambridge Analytica, a

data consultant, which used it to target Facebook users with political messaging in the 2016 presidential election. The Attorney General sought to learn whether Facebook enforced its policies restricting third-party app developers from selling or disclosing Facebook user data, and to learn whether other app developers misused Facebook user data in a manner that might violate the Consumer Protection Law. A1/21 (¶ 4). In November 2018, the Attorney General issued a Civil Investigative Demand ("CID") under G.L. c. 93A, § 6 to Facebook. The CID sought, as relevant here, the identity of apps and developers that Facebook was then investigating for potential violation of its user data policies. A1/54, 62-64. There is no other source of these facts other than Facebook, and this evidence is central to the Attorney General's investigation of whether the personal data of Massachusetts consumers has been sold or disclosed. A1/44 (¶ 68).

Through a series of communications over nine months, Facebook objected to producing the information on grounds it was attorney work product and/or within the attorney-client privilege. A1/39-43; A1/426-480. Facebook did not move for a protective order or to set aside any aspect of the CID as required by G.L. c. 93A, § 6(7). A1/44 (¶ 66).

On August 15, 2019, the Attorney General filed a Petition under G.L. c. 93A, § 7 in Suffolk Superior Court to compel compliance with the CID. A1/22

(¶ 7); A1/45 (¶ 71). The Petition sought to enforce the CID's demands for (1) the identity of, and factual information about, apps or developers that Facebook determined to examine for potential misuse of user data (referred to as "Contested Requests 1-5" in the Order on appeal), and (2) Facebook's internal communications about those apps and developers ("Contested Request 6"). A2/185-186. In response, Facebook asserted that all of the requested information was attorney work product and protected by attorney-client privilege because it was gathered in the course of the ADI, which involved Facebook's outside and in-house counsel. *Id*.

On January 16, 2020, the Superior Court granted the Attorney General's Petition, in part, ordering production in response to all Contested Requests within 90 days but allowing Facebook to withhold specific communications over which Facebook claimed the attorney-client privilege, provided it substantiate the privilege through a privilege log.[1] A2/196. Facebook filed a notice of appeal on

[1] After the Superior Court and a Single Justice of the Appeals Court denied Facebook's motion for a stay pending appeal, Facebook began producing information under the Superior Court's Order. It has also served two privilege logs in Response to Contested Request 6—one it called a "categorical" log describing seven excluded categories of documents and withholding 40,108 documents, and another 81-page log with 947 entries.

February 4, 2020. A2/197. This Court granted Facebook's application for Direct Appellate Review on May 13, 2020.

STATEMENT OF FACTS

Facebook and the Facebook Platform

Facebook is a social networking website and mobile application that allows billions of consumers worldwide ("users") to create personal profiles and connect with other users ("Friends") on mobile devices and personal computers. A1/23 (¶¶ 12-13). Users may post information on their Facebook account, engage with other users, and share personally-identifying information with other users and their Friends, including their name, date of birth, gender, current city, hometown, occupation, religion, interests, political affiliation, education, photos and/or videos. A1/23-24 (¶ 14). Users also generate data as they interact with other users, such as by commenting on other users' photos, viewing Facebook pages, or otherwise interacting with Facebook services. *Id*.

Facebook also operates its "Platform," a technological infrastructure on which Facebook allows third-party software app developers to promote and offer apps that integrate with Facebook and interact with Facebook users. A1/24 (¶ 15). By Facebook's calculation, allowing apps on its Platform was "key to increasing user engagement," which enhanced the Platform's attractiveness to advertisers that

paid Facebook for ad placement. A1/25 (¶ 18). *See* A1/97 (2012 SEC Registration Statement).

To attract developers to the Platform, Facebook offered them access to a rich stream of personally-identifying data about its users and their activity on Facebook. A1/24 (¶ 15). From 2012 through April of 2015, Facebook operated "Version 1" of the Platform, which allowed app developers to access and obtain data from the Facebook accounts of users who installed an app, *and* data from the accounts of the user's Friends who had *not* installed or engaged directly with the app.[2] A1/24-25 (¶¶ 16-17). As of March 31, 2012, over nine million apps and websites had access to the Facebook Platform. A1/25 (¶ 19); A1/100.

Facebook's Promises Regarding the Protection of User Data

Since 2012, Facebook has posted a variety of policies, terms, and conditions that governed the use of Facebook and the Platform by users and developers. A1/26-28; A1/113-171. Through them, Facebook made promises and representations to users regarding what Facebook permitted and prohibited app

[2] Facebook permitted this data sharing by default; users had to adjust their account settings to prevent it. A1/24 (¶ 16). By May 1, 2015, Facebook transitioned all developers to "Version 2" of its Platform, which restricted developers' ability to obtain the data of Friends of users that installed an app, but still permitted developers to access personal data from the Facebook user that installed the app, subject to a variety of terms and conditions. A1/25-26 (¶ 20); A1/106-108.

developers from doing with user data. For example, in late 2012 Facebook told users that "[y]our privacy is very important to us," A1/114, and assured users that, if one of their Friends installed an app, and that app took the user's data, Facebook only permitted the developer to use it "in connection with the person [i.e., Friend] that gave the permission, and no one else." A1/149 (2012 policy); A1/165-166 (2013 policy). Facebook expressly prohibited developers from selling user data to third parties, allowing them to "only request the data you need to operate your application." A1/116 (2012); A1/124 (2013). As early as 2014, Facebook required app developers to "[p]rotect the information you receive from [the Platform] against unauthorized access or use." A1/129.

Facebook also represented in those policies that it took action to detect violations and enforce these restrictions against app developers. It warned developers that it enforced data use restrictions through "automated and manual" means, that could include "disabling" an app, "restricting . . . access to platform functionality," "requiring" deletion of data, "terminating" Facebook's agreements with a developer, or other actions. A1/125 (2013 policy). *See* A1/132 (2014 policy with similar representations). Facebook also warned developers that it could audit apps for compliance with its policies and demand proof of compliance,

A1/117 (2012); A1/132 (2014), and require an app to "delete user data if" the app uses the data in a manner "inconsistent with users' expectations." A1/117 (2012).

Facebook's Pre-2018 Program to Address Misuse of User Data

Since at least 2012, Facebook has claimed it had "in place an enforcement program to prevent and respond to potential developer misuse of user information" and "dedicated significant internal and external resources . . . for detecting, escalating, investigating, and combating violations of Facebook's policies" by app developers. A1/176 (July 2018 letter to Attorney General). Based on internal records that Facebook produced, without objection, in this investigation, [redacted] IA47-48. *See* IA16-17 (¶¶ 28-29). [redacted] A1/28-30; IA16-17; IA46-48 & n.4; IA96 & IA97 (each filed on impounded CD). [redacted]

[redacted] IA16-17 (¶¶28-29); IA47-48.[3] [redacted] IA64, IA81.

Facebook informed a United States Senate committee that before 2018, it engaged in "regular and proactive monitoring of apps" and investigations into "potential app violations," A1/209, and "regularly t[ook] enforcement action against apps," including, in 2017 alone, "against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the Platform." A1/201.

Facebook's Failure to Detect and Prevent the Release of Personal User Data

Media reports in March 2018 revealed that, despite its stated enforcement policies and program, Facebook failed to detect or prevent a large-scale misuse of Facebook user data by Professor Alexander Kogan, the developer of an app called "thisisyourdigitallife" ("Kogan's App"). A1/221; A1/273-274. Kogan's app invited Facebook users to complete a personality quiz that required them to permit Kogan's app to collect personal data from their Facebook accounts as well as

[3] Within the impounded appendix are more documents describing Facebook's pre-2018 practices to detect and respond to potential developer misuse of user information. *See* IA46-49, 60-95; IA96 & IA97 (both filed on CD only).

personal data of the accounts of their Friends. A1/224-225; A1/328. Using the Platform and its associated data collection tools as they were designed, Kogan extracted personal data from the Facebook accounts of not just the approximately 300,000 Facebook users who installed Kogan's App, but also from the Facebook accounts of each of the Friends of the installing users, and in this way gained access to the data of 87 million Facebook users. A1/219.

Having obtained this trove of personal data, Kogan then sold some or all of it, in direct violation of Facebook's policies prohibiting the sale or transfer of Facebook user data, to a data analytics and advertising firm, Cambridge Analytica and other affiliated entities. A1/230 (n.33); A1/232. According to public reports, Cambridge Analytica used this data without consumers' knowledge or consent to target Facebook users with political advertising during the 2016 Presidential election. A1/271.

Facebook's 2018 Program to Address Misuse of User Data

Media reports of the Cambridge Analytica incident generated widespread concern from the public, lawmakers, and regulators about Facebook's failure to prevent misappropriation of user data from its Platform. A1/34. In response to this public outcry, Facebook and its CEO admitted that Kogan's sale of consumers' data to Cambridge Analytica violated Facebook's policies, was a "breach of the

trust people place in Facebook to protect their data," and may not have been an isolated incident. A1/331-332. *See* A1/328-329. In a posting on its website on March 21, 2018, Facebook announced that it was launching an investigation, now referred to as the "App Developer Investigation," or "ADI," by which Facebook would "crack[] down on platform abuse" by

> investigat[ing] all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access, and we will conduct a full audit of any app with suspicious activity. If we find developers that misused personally identifiable information, we will ban them from our platform.

A1/331-332. Facebook emphasized that it was undertaking the ADI and similar actions to meet its "responsibility to everyone who uses Facebook to make sure their privacy is protected. That's why we're making changes to prevent abuse." *Id*.

In describing the ADI to Congress, Facebook CEO Mark Zuckerberg said it was a step Facebook was taking "to make sure what happened with Kogan and Cambridge Analytica doesn't happen again." A1/341-342. In a letter to state Attorneys General, Facebook described the ADI as an "additional commitment[] to address data privacy concerns." A1/233. Similarly, in its 10-Q report filed with the U.S. Securities and Exchange Commission in April 2018, Facebook said the ADI involved "significant investment[] in safety [and] security" and included

"efforts to combat misuse of our services and user data by third parties." A1/374. And, in a September 2019 post on its website, Facebook "provide[d] an update on [its] ongoing App Developer Investigation," reaffirming that the ADI's "goal is to bring problems to light so [it] can address them quickly, stay ahead of bad actors and make sure that people can continue to enjoy engaging social experiences on Facebook while knowing their data will remain safe." A2/70, 72.

Facebook also outlined, for the public, Congress, and the Attorney General, the methods it was using in the ADI to uncover wrongdoing. It described two phases for identifying apps that may have misused data. A1/337 (May 2018 website post); A2/70-71 (September 2019 post); A1/350 (June 2018 responses to questions from Senate committee); A1/430 (communication to Attorney General). According to Facebook, in "Phase One" the DevOps team, "at the direction of counsel," looked for patterns or signals of misuse by an app or app developer, including an examination of information about an app, "such as the developer's identity and associations; the app's past and present names; type of app; the app's URL; and available information about the app's historical usage." A1/430. "Phase Two" includes "[e]nhanced [e]xamination" (including through "background information" and "technical" investigations) of certain apps that based on the findings of Phase One, "may have potentially engaged in misuse of Facebook user

data," such as "signals of unauthorized or disproportionate data collection, broad data requests, storage of data longer than permitted under policy, and other related issues."[4] *Id*.

Facebook promised to keep the public, Congress, and the Attorney General apprised of the progress of the ADI and to identify apps that it discovered had engaged in data misuse. In announcing the ADI on March 21, 2018, Facebook promised it would "tell people [who were] affected by apps that have misused their data" and that "moving forward, if we remove an app for misusing data, we will tell everyone who used it." A1/332-333. Its CEO made the same commitment in April 11, 2018 testimony before Congress. A1/342 (if Facebook finds during the ADI "that someone is improperly using data, we'll ban them and tell everyone affected").[5]

[4] Facebook later described the ADI as comprising three phases: "a systematic review of metrics about apps and developers," followed by "Enhanced Examination," and then "Enforcement." A1/473-480; IA163-170.

[5] Facebook reiterated this promise to its users in May 2018. A1/337 (announcing on May 14, 2018 that "[w]here we find evidence that" apps being investigated in the ADI "did misuse data, we will ban them and notify people . . . ."). It did the same in May and June when responding to post-hearing questions from two U.S. Senate committees. A1/204, A1/208, A1/350, A1/363. And Facebook also promised a group of state Attorneys General that it would "[r]eview our platform" through the ADI and "[t]ell people about data misuse." A1/233.

Over the ensuing months, Facebook released information about the progress and results of the ADI, describing the numbers and names of apps and developers it had suspended as a result. This included at least four updates to the Attorney General's Office. A1/378-386; IA105-113 (May 2018, identifying 235 suspended apps); A1/388-402; IA115-129 (June 2018, identifying 425 suspended apps); A1/434-444; IA131-141 (July 2018, identifying 68,998 suspended apps); A1446-453; IA143-150 (May 2019, identifying 176 suspended developers). It similarly identified suspended apps to members of Congress in June 2018, A1/359, A1/362-363, A2/40, and committed to keep Members updated on "future developments" from the ADI. A1/350, A1/364.

In August 2018, Facebook likewise disclosed to the public the name of an app it banned as a result of the ADI, and announced that "[s]ince launching [the ADI]," the Company had "investigated thousands of apps" and "suspended more than 400 due to concerns around the developers who built them or how the" app may have used user data. A2/9-10. Facebook promised it would "continue to investigate apps and make the changes needed to our platform to ensure that we are doing all we can to protect people's information." *Id*. In a September 2019 update on the ADI posted on its website, Facebook reported that it had made "meaningful

progress" and had "addressed millions of apps" and suspended "tens of thousands . . . for a variety of reasons." A2/70-71.

Attorney General's Investigation

The Attorney General opened a civil investigation under G.L. c. 93A, § 6 into Facebook in March 2018. Among other things, the investigation sought to determine whether any other apps (in addition to Kogan's App) misused Facebook user data, the extent of misuse, and to assess whether Facebook acted consistently with its commitments to users in its policies (as described *supra* at 12-13). The investigation also seeks information to identify other potential targets (e.g., other app developers) for investigation or enforcement action for violations of the Consumer Protection Act. A1/36-37 (¶¶ 52-54).

The Attorney General issued three Civil Investigative Demands, A1/37 (¶¶ 53-54); A1/39-41 (¶¶ 57-58), including the CID challenged in this appeal. A1/54-73. Among other things, the CID demanded the identity of the apps that Facebook reviewed in Phase One of the ADI. A1/62 (Request 1). It also sought facts about those apps, such as the app's developer, the number of users that installed the app, the data the app had permission to obtain, and the initial source of concerns about data misuse by that app. *Id.* (Request 2). The CID also demanded that Facebook identify which of the Phase One apps were subject to an "in-depth

review," "Background Information Investigation," or "Technical Investigation," respectively, as part of Phase Two of the ADI. *Id*. (Request 3(a-c)). Finally, the CID demanded that Facebook produce internal communications from January 1, 2010 onward regarding the apps identified in Requests 1, 2, and 3(a)-(c). A1/64 (Request 6, also referred to as "Contested Request 6" in the Superior Court's decision).

Facebook refused to comply with these demands. By letter dated December 4, 2018, Facebook asserted that the information was protected as attorney work product and by the attorney-client privilege. A1/456-457. In discussions and correspondence over the ensuing months, A1/42 (¶ 62), Facebook identified five categories of apps that it determined in the ADI had characteristics suggesting data misuse, and which are responsive to Requests 1, 2(a)-(h), and/or 3(a)-(c) of the CID. These categories describe the apps for which the Attorney General now seeks information and are referred to as "Contested Requests 1-5" in the Superior Court's decision. *See* A2/185-186. The five contested categories consist of apps and/or developers: (1) with a large number of installing users and permissions to obtain certain kinds of user data; (2) that, based on Facebook's "past investigative experience," present elevated risk of potential policy violations; (3) that were reported to Facebook, or identified by media reporting or inquiries, or other

referrals from internal Facebook teams; (4) for which Facebook has conducted a "detailed background check"; or (5) for which Facebook has conducted a "technical review." A1/43 (¶ 63(a)-(e)); A1/470, A1/476-478, IA160-161, IA166-168.

Although Facebook refused to comply with these requests, it did not move for a protective order or to set aside any aspect of the CID as required by G.L. c. 93A, § 6(7). A1/44 (¶ 66). Nor did Facebook provide a privilege log identifying withheld communications and substantiating its assertion of attorney work product and/or attorney-client privilege. Consequently, on August 15, 2019, the Attorney General filed her petition to enforce the CID.

The Decision and Order

On January 26, 2020, the Superior Court granted the Petition, in part. A2/196. In its decision, the Court concluded that the information from the ADI called for in the Contested Requests was not "prepared in anticipation of litigation" because it "would have been created 'irrespective of the prospect of litigation.'" A2/192, citing *Comm'r of Rev.* v. *Comcast Corp.*, 453 Mass. 293, 318-319 (2009).

To reach that conclusion, the Court assessed in detail the "history of Facebook's app policing and enforcement efforts" since 2012, and its "many public statements concerning the purposes behind its present ADI." A2/191. Based

on that evidence, the Court found "nothing materially different between the goals of the ADI" and Facebook's "historical app enforcement program," and concluded "that the ADI is just another iteration of" Facebook's "normal business operations" to review Platform apps for policy violations. *Id*.

The Court also found that even if the requested information was attorney work product, it is "indisputably factual information" (i.e. the identities of, and information about, apps) that does not reveal attorneys' "mental impressions, conclusions, opinions, or legal theories." A2/192-193. As such, any work product protection was overcome because the Attorney General had a "substantial need" for the information and could not obtain it through other means. A2/193, citing Mass. R. Civ. P. 26(b)(3).

The court also rejected Facebook's blanket assertion of the attorney-client privilege for all information sought in the Contested Requests. The court found that "Facebook has not met its burden of proving that *all* internal communications generated in course of the ADI fall within the scope of the attorney-client privilege." A2/194. Specifically, it found that "Facebook cannot conceal [the facts sought by] the Attorney General simply by sharing them with its attorneys." *Id*. Additionally, the Court ruled that Facebook's sweeping assertion of privilege over the "inner-workings of the ADI also is at odds with how [Facebook] has portrayed

the ADI publicly," specifically that Facebook "touted the ADI" as "an investigation and enforcement program undertaken for the benefit of [its] users" and "pledged to share information of suspected data misuse uncovered in the course of the ADI with" users. *Id.*

Accordingly, the Superior Court ordered Facebook to produce all materials "reasonably responsive" to Contested Requests 1-5. A2/196. The court also ordered Facebook to produce the communications sought by Contested Request 6, but disavowed any "intention to order the production of" privileged communications "based on the current record." A2/195-196. The Superior Court thus permitted Facebook to withhold communications it claims are privileged, provided it produce a privilege log "identifying each document withheld and the basis for the assertion of the privilege with sufficient factual detail" to allow the Attorney General to challenge the assertion of privilege. A2/196 (¶ 3). This appeal followed.

SUMMARY OF THE ARGUMENT

Facebook failed to carry its burden to establish that the work product doctrine precludes disclosure to the Attorney General of information about apps that were reviewed in the ADI. At the threshold, Facebook failed to prove that the requested information was "prepared in anticipation of litigation or for trial."

Mass. R. Civ. P. 26(b)(3). To do so, Facebook had to show that the information was prepared "because of" the prospect of litigation, which it could not do. *Infra* 28-36. The contemporaneous record showed, instead, that Facebook publicized the ADI as part of an effort restore trust in Facebook's ability to protect user privacy in the face of widespread public reports that it had failed to do so. Facebook's public statements demonstrate that the ADI was a critical part of its plan to improve the safety of its Platform going forward and to regain users' trust, and not an "attorney-driven" effort to assess company liabilities. In addition, as the court found, the ADI would have been done "irrespective of the prospect of litigation" because it was continuation of Facebook's long history of app enforcement activities, which it had carried out since 2012 as part of its normal business operations. Facebook cannot convert these ongoing business practices into attorney work product by delegating them to counsel in the ADI.

At most, the requested information about third-party apps is "fact" and not "opinion" work product that the Superior Court correctly ordered disclosed. Even if the ADI materials were "prepared in anticipation of litigation," the Attorney General was entitled to disclosure because she showed "a substantial need of the materials"—which are central to her investigation of a widespread breach of consumer privacy—and she is unable to obtain their "substantial equivalent"

because only Facebook has the information. Disclosure of the identity and facts about the millions of apps that Facebook was investigating at various phases in the ADI provides no meaningful glimpse into counsels' litigation strategy or opinion.

Facebook also failed to demonstrate that the attorney-client privilege precludes disclosure of all materials responsive to the Contested Requests. With respect to Contested Requests 1-5, the privilege does not preclude disclosure of information and data about apps that were reviewed in the ADI because these are not client-attorney communications made confidentially to seek legal advice. Instead, these requests seek purely factual information developed in Facebook's highly publicized ADI. Indeed, Facebook kept the public, lawmakers and regulators apprised of the progress of the ADI and publicly identified apps that misused users' personal data. Because these actions were taken to restore public trust in Facebook, they undermine its contention that the ADI is cloaked in privilege. Thus, the results of the ADI are not protected even if provided to counsel as part of the process.

And, with respect to Contested Request 6, the court correctly held that Facebook's categorical objection to producing *any* internal communication was inadequate because Facebook had the burden to specifically identify material that it believes falls within the privilege and then establish the elements of the privilege

as to each document. In that respect, the order permits Facebook to withhold specific communications if it sets out a basis for each in a privilege log.

Finally, Facebook has waived its objections by failing to move to modify or set aside the CID. The failure to bring a motion pursuant to Chapter 93A, § 6(7) "constitutes a waiver by the recipient of all objections to the C.I.D." *Attorney Gen. v. Bodimetric Profiles*, 404 Mass. 152, 154 (1989). This is not a technicality: by refusing to comply with the CID while also refusing to seek a judicial determination of its objections, Facebook has delayed this important investigation for years and forced the Attorney General to seek judicial intervention to compel Facebook's compliance. This stratagem contravened the express design of the statute to require prompt adjudication of CID objections to promote the efficacy of consumer protection investigations.

ARGUMENT

I. Facebook Has Not Met Its Burden to Establish Work Product Protection.

The work product doctrine provides a qualified protection to documents that were "prepared in anticipation of litigation or for trial." Mass. R. Civ. P. 26(b)(3). Despite stating publicly that the App Developer Investigation was initiated to "crack[] down" on data misuse and protect user privacy, Facebook now argues that

the ADI was initiated because of a threat of litigation following the Cambridge Analytica incident and is therefore protected as attorney work product. The Superior Court was right to reject Facebook's argument as unsupported by the evidence.

In evaluating whether the materials requested in the CID were prepared in anticipation of litigation, the Superior Court applied this Court's settled test: whether, "in light of the nature of the document and the factual situation in the particular case," the material can "be fairly said to have been prepared because of the prospect of litigation." A2/189, quoting *Comcast*, 453 Mass. at 317. Under that test, a document is not "prepared in anticipation of litigation" if it "would have been created 'irrespective of the prospect of litigation.'" *Id*., quoting *Comcast*, 453 Mass. at 318-319. This, the court observed, denies protection to materials "prepared in the ordinary course of business or that would have been created in essentially similar form irrespective of the [prospect of] litigation." *Id.*, quoting *United States* v. *Adlman*, 134 F.3d 1194, 1202 (2nd Cir. 1998). As set forth below, the ADI was not undertaken "because of" the prospect of litigation but was, instead, part of Facebook's highly publicized effort to regain public trust in its ability to protect user data and, at bottom, was a continuation of similar programs Facebook had undertaken in prior years to detect and prevent misuse of user data.

A. The Identity of Apps That Facebook Was Investigating for Potential Misuse of User Data, and Background Facts About Those Apps, Was Not Information Prepared "Because of" the Prospect of Litigation.

The record evidence convincingly shows that the App Developer Investigation was not "prepared in anticipation of litigation or for trial." Mass. R. Civ. P. 26 (b)(3). Although Facebook asserts that the ADI was an exception to its ongoing enforcement of data use policies against app developers, and driven "because of" litigation concerns, the Superior Court detailed the significant evidence disproving that assertion. A2/189-192.

First, the purpose of the ADI was to improve the Platform and remedy the loss of user trust in it as a result of the Cambridge Analytica incident. Facebook announced the ADI in direct response to media reports about Cambridge Analytica, which had caused widespread concern about Facebook's ability to prevent misuse of users' personal data and the safety of the Platform. A2/181-184, A2/191-192. In March 2018, Facebook publicly announced how it was addressing the issue, including by investigating and auditing apps through the ADI, banning uncooperative developers, and imposing new restrictions on access to consumer data.[6] CEO Mark Zuckerberg told users that these actions would "secure our

[6] *See, e.g.*, A1/233, A1/341-342, A1/328-329, A1/332, A1/374, A2/9-10, A2/72, A2/181-184.

platform further and make our community safer for everyone going forward." A1/329, A2/182. In a website post, Facebook announced the ADI as one "important step[] for the future of [its] platform" to "prevent abuse" and to uphold its stated "responsibility to everyone who uses Facebook to make sure their privacy is protected." A1/331-332.

In the ensuing months, Facebook continued to tout the ADI as an initiative to improve the Platform, protect users' privacy, and regain public trust. *See, e.g.*, A1/341-342 (Zuckerberg Congressional testimony); A1/233 (letter to state Attorneys General describing the ADI as an "additional commitment[] to address data privacy concerns"). Facebook specifically promoted the ADI to its investors as one of several "significant investments in safety, security, and content review efforts" the company was taking "to combat misuse of our services and user data by third parties . . . ." A1/374. Facebook later updated the public on the progress of the ADI and identified apps or developers that it had "suspended" from the Platform for violating its data use policies. A2/194.[7] In doing so, Facebook

[7] *See e.g.*, A1/350, A1/359, A1/362-364, A2/40, A2/42-43, A2/46 (letters to Congressional committees describing the ADI and identifying developers whose apps Facebook suspended as a result); A1/378-402, A1/433-451, IA105-150 (identifying suspended apps to the Attorney General); A2/9-10, A2/70-71(website posts on ADI and suspended apps).

reaffirmed that the ADI's "goal is to bring problems to light so [it] can address them quickly, stay ahead of bad actors and make sure that people can continue to . . . know[] their data will remain safe." A2/72.

Second, the ADI was just one iteration in a continuing effort by Facebook to detect policy violations by app developers and take enforcement action in response. This work was done "irrespective of the prospect of litigation." *Comcast*, 453 Mass. at 318-319. As the Superior Court found, since 2012, well before the ADI, Facebook sought to enforce policies prohibiting app developers from misusing personal user data obtained from the Platform, and did so "as part of its normal business operations." *See* A2/191.[8] Facebook reported to Congress that, prior to 2018, it engaged in "regular and proactive monitoring of apps," conducted investigations into "potential app violations," and "regularly [took] enforcement action against apps," and that in the year prior to the ADI, it took enforcement action against approximately 370,000 apps. A1/201, 209. And, earlier in the Attorney General's investigation, Facebook produced materials

[8] *See, e.g.*, A1/114, 116, 117 (Dec. 2012 policy); A1/124, A1/125 (§ V) (Feb. 2013 Platform Policy); A1/129, A1/132 (¶ 16) (July 2014 Platform Policy); A1/149 (Dec. 2012 Data Use Policy); A1/165-166 (Nov. 2013 Data Use Policy). *See also* A1/176, IA44 (stating that prior to the ADI, Facebook maintained "an enforcement program to prevent and respond to potential developer misuse of user information").

reflecting these pre-2018 enforcement practices.[9] Facebook's own CEO noted in 2018 that Facebook had "already [taken] the most important steps a few years ago in 2014 to prevent bad actors from accessing people's information" but acknowledged "there's more [it] need[ed] to do" and announced the ADI as a continuation of those efforts, i.e. a "next step[] [it] must take to continue to secure [its] platform." A1/328-329.

Based on this "largely undisputed" evidence, the Superior Court found "nothing materially different between the goals of the ADI" and Facebook's "historical app enforcement program," and "normal business operations" to review Platform apps for policy violations. A2/178; A2/191. It concluded that Facebook "pursued its ongoing app enforcement program from 2012 to the present, not for reasons of litigation or trial, but rather because [it] has made a commitment, and has a corresponding obligation to protect the privacy of its users." A2/192.

[9] *See, e.g.*, A1/28-30; IA16-17 IA46-49 ; IA60-83 ; IA96 & IA97 ; IA64

Against this body of contemporaneous evidence, Facebook submits only the declaration of its counsel prepared for this case. Among other things, counsel avers that the impetus for the ADI was to determine the legal liabilities associated with Version One of the Platform in the face of expected litigation following the Cambridge Analytica incident. A2/48-49 (¶ 4). But this assertion is at odds with Facebook's own description in the 2018 announcement and as reiterated to lawmakers, Attorneys General and the public. *See supra* at 16-21. Even if, as the declaration asserts, the ADI also enabled Facebook to consider potential liabilities, it was nonetheless designed, like Facebook's prior enforcement efforts, to identify apps that misused user data and to assure consumers that their data was safe. As the trial court concluded: "Facebook, as part of its normal business operations, has been engaged in a continuous review of Platform apps for possible violations of its Policies since 2012, and . . . the ADI is just another iteration of that program." A2/191.[10]

[10] Facebook is wrong to suggest that the Superior Court could not consider whether Facebook would have investigated app developers "irrespective of the prospect of litigation." Facebook Br. 44. This factor is central to the work product analysis. *See Comcast*, 453 Mass. at 318-319. As explained by the Second Circuit (whose "because of" test this Court adopted in *Comcast*), because the law generally favors disclosure, the work product doctrine should not shield "documents that are prepared in the ordinary course of business or that would have been created in essentially similar form irrespective of the litigation," even if "such documents

(footnote continued)

The fact that, in 2018, Facebook introduced attorneys into its program to investigate app developers does not categorically confer work product protection on ADI materials. *See* A2/50 (¶ 8) (asserting that attorneys "designed, managed, and overs[aw]" the ADI). As found by the Superior Court, "Facebook 'may not shield [its] investigation' behind the work product doctrine 'merely because . . . [it] elected to delegate . . . [its] ordinary business obligations to legal counsel." A2/192 n.4, quoting *Lumber* v. *PPG Indus., Inc*., 168 F.R.D. 641, 646 (D. Minn. 1996). *See In re Premera Blue Cross Customer Data Sec. Breach Litig*., 296 F. Supp. 3d 1230, 1246 (D. Or. 2017) (consultant's investigative report of data breach not protected where it was performed as part of ongoing services and where "the only thing that changed" was that consultant was "directed to report directly to

---

might also help in preparation for litigation . . . ." *U.S.* v. *Adlman*, 134 F.3d 1194, 1202 (2d Cir. 1998).

In considering this factor, the Superior Court did not rely on "pure speculation" or information "at odds with the undisputed record." Facebook Br. 46. Instead, its decision is firmly grounded in "the long history of Facebook's app enforcement efforts," which the court reasonably concluded would continue "irrespective of the prospect of ligation" that might follow the Cambridge Analytica disclosures. A2/180, 191-192 & n.4.

outside counsel and to label all of [its] communications as 'privileged,' 'work product,' or 'at the request of counsel'").[11]

In sum, Facebook's claim that the information sought by the Contested Requests was prepared "because of" litigation is contradicted by the substantial record evidence. Facebook's own statements and documents show the purposes of the ADI was to restore Facebook users' trust in the Platform after the reports of the Cambridge Analytica incident, and that the ADI was a continuation of an ongoing effort by Facebook to enforce its Platform policies and protect users' privacy.

B. At Most, the Material Is Fact Work Product That May Be Disclosed to the Attorney General.

The Contested Requests seek facts—the identity of and information about apps that Facebook investigated in the ADI—and not "the mental impressions, conclusions, opinions, or legal theories" of counsel. Mass. R. Civ. P.26(b)(3). Even if "prepared in anticipation of litigation," this information falls within the

[11] Similarly, courts have repeatedly held materials generated in the course of internal investigations are not work product, even if a lawyer is involved, where those investigations would have occurred irrespective of the prospect of litigation. *See, e.g.*, *Banneker Ventures, LLC* v. *Graham*, 253 F. Supp. 3d 64, 72 (D.D.C. 2017) (lawyers' witness interview memoranda prepared during internal investigation not work product because defendant would have conducted investigation absent threat of litigation); *Gillespie* v. *Charter Commc'ns*, 133 F. Supp. 3d 1195, 1201 (E.D. Mo. 2015) (reports generated at the direction of counsel during internal investigation not work product where reports were part of ongoing course of internal compliance program).

"less-shielded category" of "ordinary" work product, not within the "highly protected category" of "opinion" work product." *In re San Juan Dupont Plaza Hotel Fire Litig.*, 859 F.2d 1007, 1015-1018 (1st Cir. 1988). *See Comcast*, 453 Mass. at 314. These facts are discoverable "if the party seeking discovery demonstrates 'substantial need of the materials' and that it is 'unable without undue hardship to obtain the substantial equivalent of the materials by other means.'" *Comcast*, 453 Mass. at 314, quoting Mass. R. Civ. P. 26(b)(3).

Facebook implicitly accepts, as it must, that the CID seeks facts, not opinions of counsel. Nonetheless, it asserts that compliance would disclose "selections and compilations" of information that "exist[] only as a result of analyses involving attorney-derived criteria and judgment about legal risk." Facebook Br. 52. None of the selection criteria that Facebook has disclosed to the Attorney General for including an app in the ADI reflects counsels' opinions or analysis. Rather, the selection criteria are meant to identify "signals of potential misuse of user data," A1/430, substantially the same standard used by Facebook prior to the ADI, when attorneys were not involved. *Compare* A1/430 (ADI "systematically" reviewed apps that "had access to large amounts of user data," "to evaluate potential signals that may suggest misuse of user data," by examining, for example, the "developer's identity and associations . . . and available information

about the app's historical usage") *with* IA47-48 [redacted] For this reason, identifying which apps matched the ADI criteria for investigation would not reveal an attorney opinion.[12]

In addition, to be treated as "opinion" work product under the "selection and compilation" theory, the disclosure must "create[] a real, nonspeculative danger of revealing the lawyer's thoughts." *San Juan Dupont Plaza Hotel*, 859 F.2d at 1015. *See Cahaly* v. *Benistar Prop. Exch. Trust Co.*, 85 Mass. App. Ct. 418, 425 (2014) (work product doctrine "principally guards against disclosing attorney's strategies and legal impressions" (citation omitted)). The Superior Court correctly concluded that disclosing the "identity of the specific apps, groups of apps, and app developers that have been subjected to a 'detailed background check' or 'technical review'" in the ADI would not reveal the attorneys' thoughts. A2/193. This is especially true where Facebook has already informed the Attorney General of the general attributes, criteria, and processes it is using to identify and prioritize apps for inclusion in the ADI through its oral briefings, letters, and productions of

[12] That Facebook's position is an outlier is reflected in *Upjohn Co.* v. *United States*, 449 U.S. 383, 387-388 (1981), where Upjohn *voluntarily* provided the government the identities of employees who were interviewed during the company's internal investigation, so that IRS investigators could question them, and withheld only counsel's own notes of their own interviews.

documents.[13] A1/427-432; A1/470; A1/473-479; IA160; IA162-169. *See* *McCarthy* v. *Slade Assocs*., 463 Mass. 181, 200-201 (2012) (finding that identification of certain documents viewed by attorney "reveals nothing about the attorney's . . . opinion or impression of any of the documents, or any conclusions" of the attorney and thus were fact work product). Moreover, because Facebook is examining approximately seven million apps in the ADI,[14] A1/470, it is especially unlikely that the requested disclosures would reveal attorney opinions. Facebook cites no case that has treated factual material of this scope and magnitude as opinion work product, and many cases have refused to do so.[15]

---

[13] In addition, Facebook has, without objection, provided the Attorney General with cease and desist letters it sent to app developers that it believes may have violated its policies, and lists of apps that it has suspended from the Platform as a result of the ADI. A1/41 (¶ 59); A1/475. As described by Facebook's counsel, the selection of these apps involved specific judgments of counsel. A2/53-54 (¶¶ 19-20).

[14] That the Contested Requests utilize Facebook's phrasing to define their scope is not, as Facebook claims, an attempt to "impermissibly . . . piggyback on the work that Facebook's counsel has undertaken." Facebook Br. 53. As reflected by the extensive negotiations leading to the Petition (*see* A1/37-43), the Attorney General used Facebook's own terminology to define the group of apps the Attorney General sought at that point in time in order to narrow the dispute and enable Facebook to respond.

[15] *See, e.g.*, *Portis* v. *City of Chicago*, No. 02-C-3139, 2004 WL 1535854, at *1-3 (N.D. Ill. July 7, 2004) (database of city arrest data compiled by plaintiffs' attorney was "ordinary" work product because "the vast number of documents catalogued virtually eliminates the possibility that defendants could discern plaintiffs'

(footnote continued)

C. The Attorney General Has a Substantial Need for the Withheld Information, Which Is Available Only From Facebook and Concerns Matters at the Center of Her Investigation.

The Attorney General has shown a "substantial need of the [requested] materials" and that she "is unable without undue hardship" to obtain their "substantial equivalent . . . by other means." Mass. R. Civ. P. 26(b)(3). "As Massachusetts's chief law enforcement officer, the Attorney General has a manifest interest in enforcing G. L. c. 93A." *Exxon Mobil Corp.* v. *Attorney Gen.*, 479 Mass. 312, 323 (2018). *See* G.L. c. 93A, § 6(1) (granting special investigative authority to the Attorney General in consumer protection cases). It is squarely within her authority to demand that Facebook identify those apps and developers that, according to its own metrics and information, may have misused consumer data. Similarly, the Attorney General is empowered to investigate whether Facebook misled consumers through its representations about its oversight and monitoring of apps on its Platform, including representations about the ADI. The information Facebook is withholding squarely bears on these central questions. Accordingly, the Attorney General has a substantial need for this information to

---

litigation strategy from the database" (internal quotation omitted)); *Disability Rights Council* v. *Wash. Metro. Transit Auth.*, 242 F.R.D. 139, 144 (D.D.C. 2007) (trial strategy could not be gleaned from the identification of documents "totaling into the thousands"); *Miller* v. *Holzmann*, 238 F.R.D. 30, 31-32 (D.D.C. 2006) (20,000 documents too large to reveal counsel's trial strategy).

answer the core questions of her investigation. *See Cahaly*, 85 Mass. App. Ct. at 425 (substantial need is shown where "the work product at issue is central to the parties' substantive claims").

There is no other source from which the Commonwealth can obtain the substantial equivalent of the withheld information without undue hardship, if at all. Only Facebook is in possession of the identity of the apps and app developers that it reviewed in the ADI, and which may have engaged in misuse of user data. And only Facebook has the other requested information, such as the kind of data each app had access to and how many users' data was potentially affected. A1/44 (¶ 68). Moreover, there is an overriding public interest in obtaining this information given that Facebook has repeatedly and publicly held out the ADI as an effective and legitimate way to identify further instances of consumer harm. *See In re Grand Jury Investigation*, 437 Mass. 340, 354 (2002) (private school investigating internal complaints of student sexual assault could not "rely on an internal investigation to assert the propriety of its actions to third parties and simultaneously . . . block third parties from testing whether its representations about the internal investigation are accurate").

Accordingly, producing the information responsive to the Contested Requests will not reveal protected attorney work product. And, in any case, the

request seeks facts, and not the lawyers' thoughts, and so must be produced because the Attorney General has a substantial need of the information and cannot obtain it elsewhere. This Court should therefore affirm the order of the Superior Court holding that Facebook failed to establish work product protection.

II. Facebook Failed to Establish That the Information Sought by the Attorney General Was Protected by the Attorney-Client Privilege.

The Superior Court correctly rejected Facebook's sweeping contention that the attorney-client privilege protects virtually all information about apps the company investigated in the ADI. Facebook seeks to shield vastly more than "confidential communications" between a client and attorney when it asserts that the identity and factual attributes about apps Facebook investigated (Contested Requests 1-5) categorically fall within the scope of the privilege. Facebook Br. 38-41. And Facebook's claim that the privilege covers *all* internal communications about those apps (Contested Request 6) is far too broad because Facebook must show, for *each* communication, that all elements of the privilege are met. A2/194-195. The Superior Court's order reinforces these settled rules for application of the attorney-client privilege and should be affirmed.

As the party asserting the privilege, Facebook has the burden to prove that all the elements of the privilege are met for each communication over which it is claiming the privilege. The elements are well known: "(1) Where legal advice of

any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived." *Comcast*, 453 Mass, at 303 (quotation omitted). Thus, Facebook's burden "extends not only to a showing of the existence of the attorney-client relationship but to all other elements involved in the determination of the existence of the privilege." *Id*. at 304 (quotation omitted). As explained below, Facebook failed to shoulder this burden in its broad objection to Contested Requests 1-6.

A. The Attorney-Client Privilege Does Not Prevent Discovery of the Factual Information Sought by Contested Requests 1-5.

The Superior Court correctly rejected Facebook's blanket assertion of the attorney-client privilege over the information sought in Contested Requests 1-5 because the "privilege does not extend to any underlying facts or other information learned by Facebook during the ADI." A2/194. The privilege shields only "confidential *communications* between a client and its attorney undertaken for the purpose of obtaining legal advice." *Suffolk Constr. Co.* v. *Div. of Cap. Asset Mgmt*., 449 Mass. 444, 448 (2007) (emphasis added). *See Upjohn Co.* v. *United States*, 449 U.S. 383, 395 (1981) (privilege "only protects disclosure of communications; it does not protect disclosure of the underlying facts by those

who communicated with the attorney"); *Chambers* v. *Gold Medal Bakery, Inc.*, 464 Mass. 383, 392 (2013) (judge "should take particular care to distinguish Gold Medal's privileged communications with [counsel]" from "underlying facts" subject to disclosure). Were it otherwise, the privilege, despite its important purpose, would overwhelm "the competing societal interest of the full disclosure of relevant evidence." *Comcast*, 453 Mass. at 304.

Contested Requests 1-5 do not seek client-attorney communications; these requests seek only factual information developed in Facebook's highly-publicized ADI, including: the identity of apps that Facebook was investigating at various stages in the ADI, the apps' developer, the number of users affected by those apps, and other similar factual attributes. A1/62-63 (CID Requests 1, 2(a)-(h), and 3(a)-(c)). As the Superior Court observed, Facebook cannot conceal these facts "simply by sharing them with its attorneys." A2/194, citing *Upjohn*, 449 U.S. at 395. *See Judge Rotenberg Educ. Ctr., Inc.* v. *Comm'r of the Dep't of Mental Retardation*, 424 Mass. 430, 457 n.26 (1997) ("work plans" shared by state agency employees with counsel were not privileged where there was no showing that information was needed for counsel to advise the department or that employees were seeking legal advice), *abrogated on other grounds*, *In re Birchall*, 454 Mass. 837 (2009). That attorneys were involved in the ADI does not render all facts developed, or even all

communications made, in that investigation privileged. *See In re Grand Jury Subpoena*, 599 F.2d 504, 511 (2d Cir. 1979) ("Participation of the general counsel does not automatically cloak the investigation with legal garb."). *Cf. Grand Jury Investigation*, 437 Mass. at 352 (recognizing, but not resolving, "difficult issues involved concerning whether and to what extent an attorney's involvement in internal investigations renders such communications subject to the attorney-client privilege.").

Facebook has not established, or even asserted, that the requested information—the identities of apps and information about them—constitutes confidential "communications" between Facebook and its attorneys made for purposes of rendering legal advice. *Suffolk Constr. Co.*, 449 Mass. at 448.[16] Instead, Facebook argues that the facts sought in Contested Requests 1-5 are inseparable from the company's communications with its counsel. But, for purposes of the attorney-client privilege, "[a] fact is one thing and a communication concerning that fact is an entirely different thing." *Upjohn*, 449 U.S. at 395 (quotation omitted). Thus, in Requests 1-5, the Attorney General may

[16] Facebook cites nothing in the record demonstrating that disclosure of the facts called for in Contested Requests 1-5 would reveal confidential attorney-client communications, made to seek legal advice. Facebook Br. 38-39.

discover what Facebook employees did and learned in the ADI even if she cannot separately obtain the contents of confidential communications by Facebook to its attorneys to obtain legal advice. None of the cases cited by Facebook stand for the proposition they advance in this appeal: that facts are categorically privileged if gathered during an internal investigation involving counsel. Rather, those cases draw the unsurprising conclusion that facts may be privileged "in the context of their inclusion within otherwise privileged [client-attorney] communications." *Gen. Elec. Co.* v. *United States*, No. 3:14–cv–00190, 2015 WL 5443479, at *2 (D. Conn. Sept. 15, 2015).[17] Those cases are inapposite here, where Contested Requests 1-5 do not seek communications but facts, and thus, are not covered by the privilege.

[17] *See, e.g.*, *Fed. Trade Comm'n* v. *Boehringer Ingelheim Pharm., Inc.*, 180 F. Supp. 3d 1, 31-34 (D.D.C. 2016) (email attachments that "summarize certain facts regarding the state of the patent litigation and describe how different settlement and litigation outcomes would affect Boehringer financially" were privileged); *Banks* v. *Office of Senate Sergeant-At-Arms*, 228 F.R.D. 24, 27 (D.D.C. 2005) (privilege covered communications where client "recounts facts so that its counsel may continue to be apprised of the developing situation and [client] SAA may receive continued advice from its attorneys"). *Cf. In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 756, 764 (D.C. Cir. 2014) (finding reports of interviews of employees conducted during internal investigation to be privileged, but cautioning that the privilege "only protects disclosure of communications; it does not protect disclosure of the underlying facts by those who communicated with the attorney").

B. Facebook's General Objection Does Not Support Its Assertion of Attorney-Client Privilege Over "All" Communications Demanded by Contested Request 6

The Superior Court properly found that Facebook had not "met its burden of proving that *all* internal communications generated in course of the ADI [and thus responsive to Contested Request 6] f[e]ll within the scope of the attorney-client privilege." A2/194. Facebook relied on the declaration of its counsel to support its position that "all" communications are privileged, but this declaration is limited to broad generalizations about Facebook's investigation. A2/47-66. Nowhere in this declaration or elsewhere in the record does Facebook provide the kind of facts, such as the sender, recipients, subject matter, or date of the requested communications, necessary for a court to substantiate a claim of privilege.[18] Indeed, the declaration does not even address internal communications that occurred before the ADI commenced, which would also be responsive to Contested Request 6. Faced with a sweeping assertion of privilege based on such a sparse record, the Superior Court properly found that Facebook failed to sustain its burden.

[18] *See*, *e.g.*, A2/59-60, ¶¶ 36-37 (describing "millions" of apps, but not enumerating, quantifying, or describing any responsive communications, their senders or recipients, their respective purposes, or dates).

The Superior Court did not, however, foreclose Facebook from asserting the privilege over any particular communication for which it could substantiate the privilege. A2/195. Instead, it allowed Facebook, in complying with its Order, to withhold and assert the privilege over particular communications responsive to Contested Request 6 if it provided the Attorney General's Office with a detailed privilege log "identifying each document withheld and the basis for the assertion of the privilege with sufficient factual detail" so that the Attorney General can "understand and challenge" the claim of privilege." A2/196 (¶ 3), A2/195.[19] *See* Mass. R. Civ. P. 26(b)(5) (requiring a party that withholds discoverable information based on privilege to "expressly make the claim" and "describe the nature" of the withheld material "in a manner that . . . will enable other parties to assess the claim."); *McCarthy*, 463 Mass. at 198 n.34 (remanding case to superior court to assess records for protected materials and noting that "[p]reparation of a privilege log . . . identifying those documents claimed to be protected . . . also would be appropriate."). Accordingly, the Superior Court did not err by rejecting Facebook's blanket assertion of privilege over the communications called for by

[19] As noted *supra* n.1, Facebook has recently produced two privilege logs pertaining to materials it has withheld on grounds of privilege. The Attorney General is still assessing the sufficiency of those logs and the stated basis for the privilege.

Contested Request 6, and ordering Facebook to serve a privilege log substantiating the privilege if it withheld any responsive materials.

C. Facebook's Extensive Public Statements About the ADI Undercut Its Assertion That the ADI Was a Confidential Process Consisting Only of Privileged Communications.

To establish the privilege, Facebook was required, among other things, to show that the materials it withheld were communications made "for the purpose of obtaining legal advice" and made "in confidence." *Suffolk Constr. Co.*, 449 Mass. at 448; *Comcast*, 453 Mass. at 305. As the Superior Court found, Facebook's public statements about the ADI undercut its effort to establish both of these elements. A2/194-195.

Facebook's claim that *all* communications within the ADI were made in confidence for the purpose of obtaining legal advice, as opposed to business purposes, is contradicted by the company's own public statements. From its inception, Facebook described the ADI to the public, to Congress, to its investors, and to state Attorneys General as an effort to meet its "responsibility to everyone who uses Facebook to make sure their privacy is protected" and to "make our platform safer." A1/332-334.[20] Facebook also promised to keep the public

[20] *See also* A1/233, A1/328-329, A1/341-342, A1/374; A2/9-10; A2/70-72.

apprised of the progress of the ADI,[21] and as it progressed provided public updates, including identifying apps that misused personal data or violated Facebook's policies.[22] Thus, "[a] quintessential element of the attorney-client privilege—the expectation of confidentiality in the results of the investigation— is absent in this case." *Grand Jury Investigation*, 437 Mass. at 352.[23] Or, as the Superior Court found, Facebook's public statements about the ADI are "at odds" with its "broad assertion of the attorney-client privilege with respect to the inner-workings of the ADI." A2/194. Where Facebook undertook the ADI to provide reassurance to the public and said, in advance, it would publicly share the results, it cannot now credibly say that the entire matter is privileged. *Grand Jury Investigation*, 437

[21] *See*, *e.g.*, A1/204-205, A1/208, A1/233, A1/332-333, A1/337, A1/342, A1/350, A1/363.

[22] *See*, *e.g.*, A1/336-338, A1/359, A1/362-363, A2/9-10, A2/40, A2/70-71.

[23] In holding that communications concerning an internal investigation were not made in confidence, *Grand Jury Investigation* did not rely solely on the fact that the party was under a statutory disclosure duty. *Cf.* Facebook Br. 31-32 & n.8. This Court also found the fact the "school touted its internal investigation to the public in an effort to explain and defend its actions" to be "[a]lso relevant[.]" *Grand Jury Investigation*, 437 Mass. at 354. Here, Facebook also touted its investigation to defend its actions, which similarly shows it was not a confidential process.

Mass. at 353 ("Communications that are intended to be conveyed to others are not privileged" (citation omitted)).[24]

Facebook's argument that it did not waive the privilege through its public statements is misplaced.[25] Facebook Br. 33. The Superior Court did not reach the issue of waiver because it found that Facebook did not establish that ADI communications were categorically made in confidence, or for the purpose of obtaining legal advice, as discussed above. The Superior Court's citation to *Grand Jury Investigation* does not imply that it found a waiver of the privilege, as that case did not reach the question of waiver either. *See* 437 Mass. at 354 n.24 (holding because "the attorney-client privilege does not exist . . . , we need not consider whether a privilege was waived . . .").

---

[24] On this point, again, the cases cited by Facebook do not support a blanket privilege. Facebook Br. 40-41. Rather, they hold only that even in an internal investigation, the privilege exists only for specific confidential communications to counsel where all elements of the privilege have been established. *See In re Gen. Motors LLC Ignition Switch Litig.*, 80 F. Supp. 3d 521, 529 (S.D.N.Y. 2015) (finding intent to keep interviews confidential where record showed attorneys gave warnings to witnesses that the purpose of the interview was to "assist in providing legal advice to New GM" and matters discussed should be kept confidential); *Koch* v. *Specialized Care Servs., Inc.*, 437 F. Supp. 2d 362, 369 (D. Md. 2005) (holding only that specific communications that were "intended to be confidential," were privileged).

[25] To be clear, it is Facebook's burden to establish that it did *not* waive the privilege as to the specific communications over which it is claiming the privilege. *See Comcast*, 453 Mass. at 304.

Facebook cannot both herald the efforts it is taking to protect consumers and hide behind the work product protection or attorney-client privilege when others seek to probe those efforts further. Facebook's claims of undertaking the ADI for consumer benefit and its repeated promises of transparency belie its claims that the ADI is also a privileged effort.

III. Facebook's Objections to the CID Should Be Deemed Waived.

Chapter 93A, § 6 empowers the Attorney General to open civil investigations and issue CIDs "whenever [she] believes a person has engaged in or is engaging in any method, act or practice declared to be unlawful by" Chapter 93A. *Attorney Gen.* v. *Bodimetric Profiles*, 404 Mass. 152, 157 (1989). This section imposes a mandatory duty of compliance. *See* G.L. c. 93A, § 7 (CID recipient "shall comply with the terms thereof unless otherwise provided by the order of a court of the commonwealth."). To avoid compliance, the recipient must affirmatively move for protection from the CID by filing a motion for a protective order "in accordance with the standards of Rule 26(c) of the Massachusetts Rules of Civil Procedure", G.L. c. 93A, § 6(7), including on grounds the information sought is covered by a privilege. *See id.* § 6(5) (CID shall not "require the disclosure of any documentary material which would be privileged" or "would not be required by a subpoena duces tecum issued by a court of the commonwealth.").

This Court confirmed in *Bodimetric* that failure of a CID recipient to affirmatively move for protection from a CID "constitutes a waiver by the recipient of all objections to the C.I.D." 404 Mass. at 154. "[R]emain[ing] passive, . . . raising legal arguments only after the Attorney General brings a motion to compel" or "[m]erely informing the Attorney General of its refusal to comply" is not sufficient. *Id.* at 155.

The return date for the CID was November 20, 2018. A1/54. Facebook never moved to modify or set aside the CID, nor did it seek or receive an extension of its time to do so. The Superior Court cited the "intensive discussions and negotiations" between the parties as reason not to find Facebook's claims of work product protection and attorney-client privilege waived under *Bodimetric*. A2/188 n.3. But Facebook's "intensive discussions and negotiations" also functioned to prevent the Attorney General from obtaining the information in a timely manner, and impermissibly "shift[ed] the burden to the Attorney General to take the next legal step." *Bodimetric*, 404 Mass. at 155. This Court should not condone this stratagem, which is contrary to the commands of chapter 93A, sections 6(7) and 7, and contrary to the public's interest.

Nor should this Court be swayed by Facebook's argument that "all CID recipients would be compelled to immediately sue the Attorney General upon

receipt of every CID for fear of losing all their objections." Facebook Br. 56. Only those CID recipients with objections and grounds capable of sustaining the "heavy burden" to set aside a CID would need to contemplate seeking a protective order. *Exxon*, 479 Mass. at 324. Facebook had multiple opportunities in the nine months between the issuance of the CID in November 2018 and the Petition in August 2019 to bring a motion under section 6(7). Indeed, as of December 24, 2018, the Attorney General's Office made clear that it disagreed with Facebook's assertion of the attorney-client privilege or work product protection and "renew[ed] [its] call for production" of the materials at issue here. A1/463-467. Despite this, Facebook still did not move for protection.

Accordingly, because Facebook failed to comply with a "procedural requirement incumbent on it as a recipient of a C.I.D. for preserving its objections," it has "waived its objections to the C.I.D." *Bodimetric*, 404 Mass. at 155.[26]

[26] The Attorney General did not "relinquish[] this argument" during oral argument. *See* Facebook Br. 55. The Attorney General made the argument in her memorandum of law in support of the Petition, A2/188 (n.3) (citing memorandum), and briefly addressed it during oral argument. A2/156-57. The Superior Court also addressed the argument in its Order. A2/188 n.3. It is properly preserved for this Court's review. *Cf.* Mass. R. App. P. 22(c)(1). The Single Justice, in denying Facebook's motion to stay, also noted that Facebook's failure to comply with the statutory procedure for seeking modification of a CID

(footnote continued)

CONCLUSION

For the foregoing reasons, the Court should affirm the Order.

Respectfully submitted,

MAURA HEALEY
ATTORNEY GENERAL

/s/ Sara Cable
Sara Cable (BBO # 667084)
Jared Rinehimer (BBO # 684701)
Assistant Attorneys General
Data Privacy and Security Division
Peter Downing (BBO # 675969)
Assistant Attorney General
Consumer Protection Division
Public Protection and Advocacy Bureau
One Ashburton Place
Boston, Massachusetts 02108
(617) 963-2827/2594/2014
sara.cable@mass.gov
jared.rinehimer@mass.gov
peter.downing@mass.gov

Date: September 30, 2020

"reduces its likelihood of success on appeal." Docket Order Regarding Entry No. 1, *Attorney General's Office v. Facebook, Inc.*, 2020-J-0148 (Massachusetts Appeals Court, Single Justice Mar. 30, 2020).

ADDENDUM

TABLE OF CONTENTS

NOTIFY

IN HAND 01.17.20 AG'S Office Notified in hand W.H. 01.17.20 (NS)

Attorney General v. Facebook, Inc.

Suffolk Superior Court Action No. 1984CV02597-BLS1

Decision and Order Regarding Attorney General's Petition to Compel Compliance with Civil Investigative Demand Pursuant to G.L. c. 93A, § 7 (Docket Entry No. 1):

On August 15, 2019, petitioner Massachusetts Attorney General Maura Healey ("Attorney General") filed a "Petition to Compel Compliance with Civil Investigative Demand Pursuant to G.L. c. 93A, § 7" (the "Petition") to compel respondent Facebook, Inc.'s ("Facebook" or the "Company") compliance with the Attorney General's Civil Investigative Demand No. 2018-CPD-67 (the "Third CID").[1] The Attorney General issued the Third CID to Facebook in November 2018 as part of its ongoing investigation into whether certain third-party applications ("apps") and app developers have improperly acquired and/or misused private information of Facebook's users. Facebook currently is engaged in its own internal investigation into the same subject matter and argues that at least some of the information requested by the Attorney General in its Third CID is protected from disclosure by the work product doctrine and/or the attorney-client privilege.

The parties have filed lengthy memoranda in support of, or in opposition to, the Petition, supported by various exhibits and declarations. On November 7, 2019, the Court conducted a lengthy hearing on the Petition. All parties attended and argued. Upon consideration of the written submissions of the parties and the oral arguments of counsel, the Petition will be **ALLOWED IN PART**, for the reasons discussed below.

Factual Background

The following facts, which are largely undisputed, are taken or derived from the Petition, Petition exhibits, and other materials submitted by the parties.

Facebook and the Facebook Platform

Facebook is a Delaware corporation which maintains its headquarters and principal place of business in Menlo Park, California. The Company also has offices in Cambridge, Massachusetts. Facebook offers an online social networking service through its website and mobile application that allows the people and other entities who use its service (generally referred to as "users" or "friends") to create personal profiles and interact with other Facebook users. Facebook has a staggering number of users. As of June 2019,

[1] Due to confidentiality concerns, the Court has, by agreement of the parties and in conformance with Trial Court Rule VIII, Uniform Rules on Impoundment Procedure, impounded certain portions of the Petition and accompanying exhibits filed by the Attorney General. Redacted copies of these materials have been made part of the public case record for informational purposes.

Facebook had more than 1.59 billion daily active user accounts, and more than 2.41 billion monthly active user accounts. Petition, ¶ 13.

Facebook users can choose to share certain personally-identifying information about themselves with other users. This information includes, but is not limited to, the user's name, date of birth, gender, current city, hometown, occupation, religion, interests, political affiliation, education, photos, and videos. Facebook users also generate data based on their activity on Facebook, such as posting comments on their Facebook profile or the profiles of other Facebook users, posting and commenting on photos, interacting with the Facebook platform, or viewing and interacting with other Facebook pages (*e.g.*, pages associated with businesses, brands, or political organizations). *Id.*, ¶ 14.

Facebook also operates the Facebook Platform (the "Platform"), which is the technological infrastructure that allows third-party app developers to create apps that integrate with Facebook and can be utilized by Facebook users. *Id.*, ¶ 15. Such apps include, among other things, games, location-based services, music-playing services, and news feeds. When a Facebook user installs and uses an app, Facebook allows the app and its developer to obtain certain personal data about the user from the user's Facebook account using software communication protocols called "Application Programming Interfaces" ("APIs"). *Id.*

From 2012 to May 1, 2015, Facebook operated "Version 1" of its Platform. Version 1 allowed apps to obtain personal data from the Facebook accounts of not only users that installed or used an app, but also allowed the apps to pull personal data from the accounts of the app user's Facebook friends who had never installed or used the app. A Facebook user's friend could disallow this type of sharing by adjusting his or her Facebook account settings, but for a period of time, Facebook set users' settings so that this type of sharing was permitted by default and changing it required an affirmative act on the part of the user's friend. *Id.*, ¶ 16. The apps generated revenue and data about users for both the app developers and Facebook itself. As of March 31, 2012, over nine million apps and websites had integrated with the Version 1 Platform.

In April 2014, Facebook announced that it was launching "Version 2" of its Platform. Version 2 restricts the scope of the user data that an app developer can access through the Platform. *Id.*, ¶ 20. In Version 2, app developers can only access certain basic information about the app user (*e.g.*, basic profile information, email address, and list of friends who also used the app), and no longer can access data about the app user's friends unless the app developer has sought and obtained permission from Facebook to obtain additional data. Facebook allowed apps a one-year grace period (until May 1, 2015) to continue operating on Version 1 of its Platform (and to continue accessing more expansive user data) before transitioning to Version 2.

Facebook's Platform Policies and Enforcement Program

At all relevant times, Facebook maintained a variety of policies, terms, and conditions that governed the use of Facebook and its Platform by Facebook users and app developers (collectively, "Facebook's Policies"). Facebook's Policies included various representations and promises to users regarding what Facebook permitted and prohibited app developers from doing with user data. For instance, Facebook's Policies: prohibited app developers from selling or licensing user data obtained from Facebook to any third party; prohibited app developers from sharing any user data obtained from Facebook with any ad network, data broker, or other advertising service; restricted app developers from accessing user data that was unnecessary for the functioning of the app; and required app developers to protect information they received against unauthorized access or use.

From 2012 to 2014, Facebook's Policies assured users that "[i]f an application asks permission from someone else [*i.e.*, the user's friend] to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, and no one else." *Id.*, ¶ 23. Facebook's Policies also warned app developers that it: "[M]ay enforce against your app or website if we conclude that your app violates our terms or is negatively impacting the Platform .... Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to platform functionality, requiring that you delete data, terminating our agreements with you and any other action that we deem appropriate." *Id.*, ¶ 24. Facebook specifically warned app developers that it had the ability to audit apps, and that they would be required to delete user data if the data was misused.

Beginning in or around 2012, Facebook, by its own admission, "put in place an enforcement program to prevent and respond to potential developer misuse of user information" (the "Enforcement Program"). *Id.*, ¶ 27. Facebook has "dedicated significant internal and external resources to this [Enforcement Program] in order to detect and investigate violations of Facebook's [P]olicies." *Id.* According to the Company, its internal "Development Operations" or "DevOps" team "has consistently played a central role in enforcing Facebook's [P]olicies and protecting user data and Facebook's Platform...." *Id.*, ¶ 28. Facebook also has stated publicly that, in the usual course of its business, it has engaged in "regular and proactive monitoring of apps" and investigations for potential app violations. *Id.*, ¶ 33.

Professor Kogan and Cambridge Analytica

In 2013, Professor Aleksandr Kogan ("Professor Kogan") from the University of Cambridge in England developed and made available a Facebook app called "thisisyourdigitallife." *Id.*, ¶ 34. Professor Kogan used his app to collect personally-identifying data from the Facebook accounts of users who installed his app, as well as

data from the accounts of each user's Facebook friends. The data collected by Professor Kogan included user names, birthdates, genders, languages, age ranges, current cities, lists of names of all of the user's friends, the Facebook pages that each user had "liked," and, for a smaller subset of users, email addresses and the content of their Facebook posts, Facebook messages, and photos. Professor Kogan succeeded in obtaining personally-identifying data from the Facebook accounts of approximately 87 million Facebook users. He then sold some or all of that data to Cambridge Analytica, a political data analytics and advertising firm, and to certain related entities, Strategic Communication Laboratories and Eunoia Technologies, Inc. According to Facebook, Professor Kogan's sale of the personally-identifying data he had collected to Cambridge Analytica and its related entities violated Facebook's Policies.

Facebook was unaware of Professor Kogan's wholesale collection and sale of its users' personal data until a media inquiry alerted Facebook to the problem in December 2015. The Company responded by demanding that Professor Kogan, Cambridge Analytica, and the related parties delete the misappropriated data, and it thereafter obtained "certifications" from these parties that the data had, in fact, been deleted. *Id.*, ¶ 37.

From December 2015 to March 2018, aside from demanding that Cambridge Analytica and its related entities delete the misappropriated user data they had obtained from Professor Kogan and "certify" that they had done so, Facebook took no enforcement action against these entities. For example, Facebook did not shut off Cambridge Analytica's access to the Facebook Platform. To the contrary, as of January 2016, the Company continued to court Cambridge Analytica's business, and it continued to allow Cambridge Analytica access to Facebook's users in order to conduct advertising campaigns on behalf of Cambridge Analytica's clients until early 2018.

In March 2018, news broke that Cambridge Analytica had not actually deleted the Facebook user data that it had obtained from Professor Kogan. Instead, Cambridge Analytica used the data to target Facebook users with campaign messaging benefiting Cambridge Analytica's clients during the 2016 U.S. Presidential Election.

The news of Cambridge Analytica's interference in the 2016 U.S. Presidential Election, using the private data that it had obtained from Professor Kogan, generated considerable attention and concern from the public, lawmakers, and government regulators. In a blog post dated March 22, 2018, Facebook Chief Executive Officer Mark Zuckerberg ("Mr. Zuckerberg") promised that the Company would take immediate action to prevent a recurrence of the problem. He said,

> First, we will investigate all apps that had access to large amounts of information before we changed our platform to dramatically reduce data access in 2014, and we will conduct

> a full audit of any app with suspicious activity. We will ban any developer from our platform that does not agree to a thorough audit. And if we find developers that misused personally identifiable information, we will ban them and tell everyone affected by those apps.
>
> Second, we will restrict developers' data access even further to prevent other kinds of abuse. For example, we will remove developers' access to your data if you haven't used their app in 3 months. We will reduce the data you give an app when you sign in -- to only your name, profile photo, and email address.
>
> . . .
>
> Third, we want to make sure you understand which apps you've allowed to access your data.

Petition, Exhibit FF.

Mr. Zuckerberg pledged that Facebook was "serious about doing what it takes to protect our community." *Id.* He said that,

> [w]hile this specific issue involving Cambridge Analytica should no longer happen with new apps today, that doesn't change what happened in the past. We will learn from this experience to secure our platform further and make our community safer for everyone going forward."

Id.

Facebook's App Developer Investigation

Consistent with Mr. Zuckerberg's pledge, Facebook launched what it now refers to as its "App Developer Investigation" ("ADI") in March 2018. Petition, ¶ 44. The Company has summarized the goals of its ADI, in relevant part, as follows,

> We will investigate all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access, and we will conduct a full audit of any app with suspicious activity. If we find developers that misused personally identifiable information, we will ban them from our platform.

Petition, Exhibit GG at 2. Facebook also has pledged to share information of suspected data misuse uncovered in the course of its ADI with its user community. Specifically, Facebook has said,

> We will tell people affected by apps that have misused their data. This includes building a way for people to know if their data might have been accessed via "thisisyourdigitallife." Moving forward, if we remove an app for misusing data, we will tell everyone who used it.

Id.

At the request of Facebook's management, the Company's in-house legal team retained the law firm of Gibson Dunn & Crutcher LLP ("Gibson Dunn") to design and direct the ADI in order to gather the facts needed to provide legal advice to Facebook about litigation, compliance, regulatory inquiries, and other legal risks facing the Company as a result of potential data misuse and other activities by third-party app developers operating on Version 1 of the Facebook Platform. See Declaration of Stacy Chen in Support of Respondent's Opposition to the Attorney General's Petition, ¶¶ 6, 8 (Docket Entry No. 29) ("From the beginning, Gibson Dunn and Facebook's in-house counsel have designed, managed, and overseen all stages of the ADI, with input of subject matter experts across the company.").

In the ensuing months and years, Facebook has periodically updated the public about the progress of its ADI. For example, Facebook issued a public statement in May 2018 which reported that "thousands of apps have been investigated and around 200 have been suspended -- pending a thorough investigation into whether they did in fact misuse any data." Petition, Exhibit HH. More recently, in September 2019, Facebook issued a further public update, which states, in part,

> We initially identified apps for investigation based on how many users they had and how much data they could access. Now, we also identify apps based on signals associated with an app's potential to abuse our policies. Where we have concerns, we conduct a more intensive examination. This includes a background investigation of the developer and a technical analysis of the app's activity on the platform. Depending on the results, a range of actions could be taken from requiring developers to submit to in-depth questioning, to conducting inspections or banning an app from the platform.

> Our App Developer Investigation is by no means finished. But there is meaningful progress to report so far. To date, this investigation has addressed millions of apps. Of those, tens of thousands have been suspended for a variety of reasons while we continue to investigate.

Transmittal Declaration of Sara Cable, Esq., dated October 28, 2019, Exhibit 1 (the "September 2019 Facebook ADI Update").

The Attorney General's Investigation

In March 2018, the Attorney General opened an investigation into Facebook's policies and protections with respect to user data under the authority granted by G.L. c. 93A, § 6. The Attorney General's decision to investigate Facebook was prompted, in part, by media reports concerning Cambridge Analytica's misuse of private Facebook user information, including private information associated with the millions of Massachusetts residents who use Facebook. Petition, ¶ 52. The Attorney General's investigation seeks, among other things,

> to identify other instances of potential misuse and consumer harm, to assess whether Facebook has acted and is acting consistently with its representations to users regarding its policies and practices to safeguard their data on the Platform, and to identify other potential targets for investigation or enforcement action.

Id.

Since commencing her investigation, the Attorney General has served Facebook with a total of three civil investigative demands ("CIDs") seeking information about, generally speaking, Facebook's policies and practices, the third-party apps that utilize the Company's Platform, Facebook's ADI, and the particular apps that Facebook has flagged as potentially problematic in the course of its ADI. The Attorney General issued her first CID to Facebook (No. 2018-CPD-25) on April 23, 2018; her second CID (No. 2018-CPD-39) on June 20, 2018; and her third CID (No. 2018-CPD-67, the "Third CID") on November 5, 2018. Both sides agree that the Attorney General's multiple CIDs have constituted an iterative process, with the focus and specificity of the requests becoming more refined as the Attorney General has gained a better understanding of the nature and workings of Facebook's ADI.

The Contested Requests

Many trees, virtual and otherwise, have given up their lives to the ensuing correspondence between Facebook and the Attorney General's Office concerning Facebook's compliance (or non-compliance) with the Attorney General's three successive CIDs. It is sufficient for present purposes to say that Facebook has produced some, but not all, of the information requested by the Attorney General. In particular, Facebook has refused, on work product and attorney-client privilege grounds, to turn over to the Attorney General certain information generated in the course of its ADI about the specific apps, groups of apps, and app developers that Facebook claims to have flagged as potentially problematic or, at the very least, has identified as worthy of additional examination. All of the information currently at issue between the parties is requested in the Attorney General's Third CID, a copy of which is appended to the Petition as Exhibit A. The specific requests at issue (the "Contested Requests") are as follows:

1. The group of 6,000 apps with a large number of installing users that is referenced in Exhibit TT and Exhibit UU to the Petition at FB-CA-MAAG-C001.005;[2]

2. The group of apps and developers that fall within certain categories that, based on Facebook's "past investigative experience," present an elevated risk of potential policy violations, as referenced in Exhibit UU to the Petition at FB-CA-MAAG-C001.004;

3. The group of apps and developers that were reported to Facebook from outside of the ADI process, such as through the Data Abuse Bounty Program (to the extent not already produced), media reporting and inquiries, and other referrals from internal Facebook teams, as referenced in Exhibit UU to the Petition at FB-CA-MAAG-C001.004;

4. The group of apps and/or developers on which, to date, Facebook has conducted a "detailed background check ... to gauge whether the app or developer has engaged in behavior that may pose a risk to Facebook user data or raise suspicions of data misuse, to identify connections with other entities of interest, and to

[2] Exhibit TT to the Petition is a copy of a June 12, 2019, e-mail message from Facebook's outside legal counsel in this matter to various representatives of the Attorney General's office. Exhibit UU is a copy of a July 1, 2019, letter from Facebook's outside counsel to Assistant Attorney General Sara Cable.

search for any other indications of fraudulent activity," as referenced in Exhibit UU to the Petition at FB-CA-MAAG-C001.006;

5. The group of apps on which, to date, Facebook has conducted a "technical review" to analyze "available technical information about the apps derived from Facebook's available internal usage records in order to gauge data collection practices -- such as the disproportionate collection of data and broad data requests -- which may suggest data misuse," as referenced in Exhibit UU at FB-CA-MAAG-C001.006; and

6. All of Facebook's internal communications and internal correspondence concerning the apps that "had access to large amounts of Facebook data before the 2014 changes to [the Company's] Platform took effect," and/or for which Facebook has conducted an "in-depth review," a "Background Information Investigation," or a "Technical Investigation."

Petition at 28 ("Prayer for Relief"), and Exhibit A at 9-11.

When further discussions between the parties concerning Facebook's willingness to produce the documents and information called for in the Contested Requests proved fruitless, the Attorney General filed her Petition to compel compliance with her Third CID on August 15, 2019.

Discussion

Section 2 of G.L. c. 93A prohibits the commission of any "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce" within the Commonwealth of Massachusetts. G.L. c. 93A, § 2. Responsibility for policing this prohibition falls, in large part, on the Office of the Attorney General. Section 6(1) of G.L. c. 93A provides that, "whenever ... [the Attorney General] believes a person has engaged in or is engaging in any method, act or practice declared to be unlawful by this chapter, [he or she] may conduct an investigation to ascertain whether in fact such person has engaged in or is engaging in such method, act or practice." G.L. c. 93A, § 6(1). See also *Harmon Law Offices, P.C. v. Attorney General*, 83 Mass. App. Ct. 830, 834-835 (2013) ("*Harmon*") (recognizing that Section 6(1) "gives the Attorney General broad investigatory powers to conduct

investigations whenever she believes a person has engaged in or is engaging in any conduct in violation of the statute"). In conducting an investigation under Section 6(1), the Attorney General may,

> (a) take testimony under oath concerning such alleged unlawful method, act or practice; (b) examine or cause to be examined any documentary material of whatever nature relevant to such alleged unlawful method, act or practice; and (c) require attendance during such examination of documentary material of any person having knowledge of the documentary material and take testimony under oath or acknowledgment in respect of any such documentary material.

G.L. c. 93A, § 6(1).

A written request for information from the Attorney General under G.L. c. 93A, § 6(1), usually takes the form of a "Civil Investigative Demand" (as before, a "CID"). Although the Attorney General may not act arbitrarily or in excess of his or her statutory authority in issuing and enforcing a CID (see *Harmon*, 83 Mass. App. Ct. at 834-835), "[t]here is no requirement that the Attorney General have probable cause to believe that a violation of G.L. c. 93A has occurred." *CUNA Mutual Ins. Soc. v. Attorney General*, 380 Mass. 539, 542 n.5 (1980) ("*CUNA*"). It is enough if the Attorney General simply believes that "a person has engaged in or is engaging in conduct declared to be unlawful" by G.L. c. 93A. *Id.* The recipient of a CID who does not wish to respond, in whole or in part, bears a "heavy burden" to show "good cause" why it should not be compelled to do so. G.L. c. 93A, § 6(7). See also *Harmon*, 83 Mass. App. Ct. at 834 (internal quotation marks and citation omitted). "Good cause" in this context means that the receiving party must demonstrate that Attorney General is "act[ing] arbitrarily or capriciously or that the information sought is plainly irrelevant." *Harmon*, 83 Mass. App. Ct. at 834-835. In making such an assessment, "it is appropriate for the judge to consider that effective investigation requires broad access to sources of information...." *Matter of a Civil Investigative Demand Addressed to Yankee Milk, Inc.*, 372 Mass. 353, 364 (1977) ("*Yankee Milk*").

In this case, Facebook's refusal to provide the documents and other materials called for in the Contested Requests is not based on any suggestion that the information requested in the Third CID is not relevant to the subject matter of the Attorney General's investigation. Rather, it is Facebook's contention that the information currently sought by the Attorney General – most of which indisputably derives from Facebook's ongoing ADI – is protected from disclosure by the work product doctrine and/or the attorney-

client privilege. Facebook argues that the Attorney General's Petition should be denied in its entirety because everything called for in the Contested Requests falls within one or both of these protected categories. The Attorney General, not surprisingly, disagrees.[3] As the legal analysis differs with respect to the applicability of the work product doctrine and the applicability of the attorney-client privilege, the Court separately addresses each of the arguments put forth by Facebook below.

I. Applicability of the Work Product Doctrine.

The work product doctrine is intended to "enhance the vitality of an adversary system of litigation by insulating counsel's work from intrusions, inferences, or borrowings by other parties." *Commissioner of Revenue v. Comcast Corp.*, 453 Mass. 293, 311 (2009) ("*Comcast*") (citation omitted). Its purpose is to "establish a zone of privacy for strategic litigation planning ... to prevent one party from piggybacking on the adversary's preparation." *Id.* at 311-312 (citations and internal quotation marks omitted).

In Massachusetts, the work product doctrine is codified in Mass. R. Civ. P. 26(b)(3), titled "Trial Preparation: Materials," which states, in relevant part, that,

> a party may obtain discovery of documents and tangible things otherwise discoverable under subdivision (b)(1) of this rule and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative (including his attorney, consultant, surety, indemnitor,

[3] The first ground upon which the Attorney General urges this Court to reject Facebook's claims of work product protection and attorney-client privilege is the Attorney General's assertion that Facebook necessarily waived its right to object to the Third CD by failing to file a motion to "modify or set aside such demand," or for a "protective order in accordance with the standards set forth in Rule 26(c)," within "twenty-one days after the [Third CID] was served" as provided in G.L. c. 93A, § 6(7). See Memorandum of Law in Support of the Attorney General's Petition to Compel Compliance with Civil Investigative Demand ("Attorney General's Memo") at 17-18, citing *Attorney General v. Bodimetric Profiles*, 404 Mass. 152, 154 (1989) ("*Bodimetric*") (holding that the failure of CID recipient to file motion pursuant to G. L. c. 93A, Section 6(7), constituted a waiver of right to object to CID). The Court perceives the situation differently. The Massachusetts Supreme Judicial Court ("SJC") warned in *Bodimetric* against "passive" non-compliance with a CID, which certainly does not fairly characterize the intensive discussions and negotiations that have taken place between Facebook and the Attorney General since (and even before) the Third CID was served in November 2018. It would be counterproductive in the grand scheme of things to require every recipient of a CID from the Attorney General to automatically commence litigation if the parties are unable to fully negotiate a mutually-acceptable response plan within twenty-one days of service of the CID. Thus, this Court reads *Bodimetric* as permitting a judge, in his or her discretion, to deem an unresponsive recipient's failure to file a timely motion for relief under G.L. c. 93A, § 6(7), as a waiver of that party's right to object to the CID. See *Bodimetric*, 404 Mass. 154-155 (analogizing the requirements of Section 6(7) to the "Federal rules," whereby a "recipient of a request for discovery who fails to move for a protective order *may be deemed to have waived his objections*") (emphasis added). The Court further exercises the discretion recognized in *Bodimetric* to deny the Attorney General's request that Facebook be deemed to have waived its objections to the Third CID in the circumstances of this case.

> insurer, or agent) only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of his case and that he is unable without undue hardship to obtain the substantial equivalent of the materials by other means. In ordering discovery of such materials when the required showing has been made, the court shall protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation.

Mass. R. Civ. P. 26(b)(3). The Massachusetts Supreme Judicial Court ("SJC"), in turn, has summarized and simplified the language of Rule 26(b)(3) by holding that work product protection extends to "(1) documents and tangible things, (2) [created] by or for another party or by or for that other party's representative (including his attorney, consultant, surety, indemnitor, insurer, or agent), and (3) in anticipation of litigation or for trial." *McCarthy v. Slade Assocs.*, 463 Mass. 181, 194 (2012) ("*McCarthy*"), quoting P.M. Lauriat, S.E. McChesney, W.H. Gordon, & A.A. Rainer, Discovery § 4:5 (2d ed. 2008 & Supp. 2011) (internal quotation marks omitted).

The critical question presented with respect to Facebook's claim of work product protection in this case is whether the documents and other materials called for in the Attorney General's Third CID were "prepared in anticipation of litigation or for trial." *Id.* A document is prepared in anticipation of litigation if, "in light of the nature of the document and the factual situation in the particular case, the document can be fairly said to have been prepared *because of the prospect of litigation*." *Comcast*, 453 Mass. at 317 (citations omitted) (emphasis added). Preparation for litigation "includes litigation which, although not already on foot, is to be reasonably anticipated in the near future." *Ward v. Peabody*, 380 Mass. 805, 817 (1980). A document is not "prepared in anticipation of litigation," however, if it would have been created "'irrespective of the prospect of litigation.'" *Comcast*, 453 Mass. at 318-319, citing and quoting *United States v. Textron Inc. & Subsidiaries*, 507 F. Supp. 2d 138, 149 (D. R.I. 2007), aff'd in part, 553 F.3d 87 (1st Cir. 2009). As plainly stated by the United States Court of Appeals for the Second Circuit in *United States v. Adlman*, 134 F.3d 1194, 1202 (2d Cir. 1998), "[i]t is well established that work-product privilege does not apply" to documents "prepared in the ordinary course of business or that would have been created in essentially similar form irrespective of the [prospect of] litigation."

The Attorney General argues here that,

> [t]he prospect of litigation was not Facebook's primary motive for attempting to identify other apps or developers

> who may, like Professor Kogan and Cambridge Analytica, have sold or misused consumer data from the Platform. Rather, as evidenced by its own public statements, Facebook launched the ADI as part of an effort to repair and enhance its public reputation in response to widespread concern and criticism by the public and government officials after the public learned about Kogan's and Cambridge Analytica's conduct in March of 2018. In announcing the ADI, Facebook made this purpose clear, admitting that because it had "seen abuse of our platform and the misuse of people's data, ... we know we need to do more," and describing the ADI as one of several "important steps for the future of our platform."

Attorney General's Memo at 19-20.

The Attorney General also asserts that Facebook's ADI,

> is not a new, isolated process put in place because of the prospect of litigation. Although Facebook has adopted the term "ADI" to describe its current app review process, it is merely the latest iteration of a process that Facebook has asserted it has maintained since at least 2012, *i.e.* "an enforcement program to prevent and respond to potential developer misuse of user information" to which Facebook has "dedicated significant internal and external resources" in order to "detect[], escalat[e], investigat[e], and combat[] violations of Facebook's policies." Facebook has similarly claimed, in response to questions from members of the Senate Judiciary Committee, that part of its regular business practices are to engage in "regular and proactive monitoring of apps" and "investigat[ing] for potential app violations," including through a "variety of manual and automated checks to ensure compliance with our policies and a positive experience for people," such as "random checks of existing apps along with the regular and proactive monitoring of apps," responding to "external or internal reports ... [of] potential app violations," and where it finds violations of its Policies, "employ a number of measures, including restricting applications from our platform, preventing developers from

> building on our platform in the future, and taking legal action where appropriate."

Id. at 21.

The Court agrees that the history of Facebook's app policing and enforcement efforts, which started no later than 2012, as well as the Company's many public statements concerning the purposes behind its present ADI, compel the conclusion that the ADI is not being undertaken by Facebook "in anticipation of litigation or for trial." Facebook assured its users when it introduced Version 1 of its Platform back in 2012 that "[y]our privacy is very important to us" (Petition, Exhibit D at FB-AG-00000142), and, as a consequence, it "put in place an enforcement program to prevent and respond to potential developer misuse of user information." *Id.*, Exhibit I at FB-CA-MAAG-NYAG-C012.01. As previously noted, Facebooks asserts that, over the years, it has "dedicated significant internal and external resources to this program, including for detecting, escalating, investigating, and combating violations of Facebook's policies." *Id.* Facebook's ongoing enforcement program has included, without limitation, "monitor[ing] abnormal app activity on the Platform via a mix of manual flags, automated signals, and random sampling to detect potential misuse of the Platform" (*id.*, Exhibit I at FB-CA-MAAG-NYAG-C012.06), as well as "regular and proactive monitoring of apps" and investigations into "potential app violations." *Id.*, Exhibit N at 121-122. In 2017 alone (*i.e.*, the year *before* the Cambridge Analytica incident came to light), Facebook claims to have taken enforcement action "against about 37,000 apps, ranging from imposing certain restrictions to removal of the app from the platform." *Id.*, Exhibit N at 6.

Compared against this factual record, Facebook's ADI is fairly described as "business as usual." There is, for sure, nothing materially different between the goals of the ADI as announced by Facebook in March 2018 (*i.e.*, to "investigate all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access," to "conduct a full audit of any app with suspicious activity," and to "ban ... from our platform" any "developers that misused personally identifiable information" (Petition, Exhibit GG)), and Facebook's historical app enforcement program, as detailed above. The record shows that Facebook, as part of its normal business operations, has been engaged in a continuous review of Platform apps for possible violations of its Policies since 2012, and that the ADI is just another iteration of that program.[4] The evidence

[4] The Court is unpersuaded, in this context, by Facebook's argument that the information and materials generated by its ADI qualify for work product protection because the ADI is a "lawyer-driven effort" that was "born amid and because of" the Cambridge Analytica incident. See Memorandum in Opposition to the Attorney General's Petition to Compel Compliance with Civil Investigative Demand Pursuant to G.L. c. 93A, § 7 ("Facebook's Opp.") at 25-26 (internal quotation marks omitted). These facts, while perhaps relevant, are not decisive. As noted above, the operative test is whether the information and materials have been "prepared in anticipation of litigation," or whether they would have been created "irrespective

also shows that Facebook has pursued its ongoing app enforcement program from 2012 to the present, not for reasons of litigation or trial, but rather because the Company has made a commitment, and has a corresponding obligation to protect the privacy of its users. See, e.g., Petition, Exhibit GG at 2 (Facebook announcement of ADI in March 21, 2018, which states, in part, "[w]e have a responsibility to everyone who uses Facebook to make sure their privacy is protected"). The Court therefore concludes that Facebook's ADI is not being conducted "in anticipation of litigation or for trial," and would have been undertaken by the Company "irrespective of the prospect of litigation." See *Comcast*, 453 Mass. at 317-318 (internal quotation marks and citations omitted). Accordingly, the fruits of that investigative and enforcement program do not qualify for work product protection under Mass. R. Civ. P. 26(b)(3).

Even if the Court were to conclude otherwise, however, that would not be the end of the story. Work product protection is qualified and "can be overcome if the party seeking discovery demonstrates substantial need of the materials and that it is unable without undue hardship to obtain the substantial equivalent of the materials by other means." *Comcast*, 453 Mass. at 314, quoting Mass. R. Civ. P. 26(b)(3) (internal quotation marks omitted). A party demonstrates a "substantial need" where "the work product material at issue is central to the substantive claims in litigation." *McCarthy*, 463 Mass. at 195 (citation omitted). See also *Cahaly v. Benistar Property Exchange Trust Co., Inc.*, 85 Mass. App. Ct. 418, 425 (2014) ("*Cahaly*"). There are, moreover, two types of work product: "fact" work product (sometimes referred to as "ordinary" work product), and "opinion" work product. *Cahaly*, 85 Mass. App. Ct. at 425. "Opinion" work product, which includes mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation, is afforded greater protection than "fact" work product, which receives "far less protection." *Id.*

The Attorney General contends that most of the materials and information called for in the Contested Requests, including information identifying the particular apps, groups of apps, and app developers as to which Facebook has conducted a "detailed background check" or "technical review," qualifies as "fact" work product. Attorney General's Memo at 23-25. The Attorney General also contends that she has a "substantial need" for the information sought, and that "[t]here is no other source from which the Commonwealth can obtain the substantial equivalent of the withheld information without undue hardship." *Id.* at 26.

---

of the prospect of litigation." See *Comcast*, 453 Mass. at 317-318 (internal quotation marks and citation omitted). Given the long history of Facebook's app enforcement efforts, the Court finds the latter to be true in this instance. In such circumstances, Facebook "may not shield [its] investigation" behind the work product doctrine "merely because ... [it] elected to delegate ... [its] ordinary business obligations to legal counsel." *Lumber v. PPG Indus., Inc.*, 168 F.R.D. 641, 646 (D. Minn. 1996).

The Court agrees with the Attorney General on both counts. The purposes of the Attorney General's current investigation of Facebook expressly include, among other things, "identify[ing] ... instances of potential misuse and consumer harm" of Massachusetts user's private information by apps operating on Facebook's Platform, as well as "identify[ing] other potential targets for investigation or enforcement action." Petition, ¶ 52. The identity of the specific apps, groups of apps, and app developers that have been subjected to a "detailed background check" or "technical review" by Facebook is indisputably factual information that is entitled to "far less" work product protection. *Cahaly*, 85 Mass. App. Ct. at 425. Furthermore, only Facebook knows the identity of these apps and developers, and there is no other way for the Attorney General to obtain this information on her own. Accordingly, even if the Court was persuaded that the fruits of Facebook's ADI qualify for work product (which position the Court has explicitly rejected), it would conclude that the Attorney General has demonstrated a "substantial need of the materials" and that she is "unable without undue hardship to obtain the substantial equivalent of the materials by other means." See Mass. R. Civ. P. 26(b)(3).

II. Applicability of the Attorney-Client Privilege.

Facebook further argues that the Attorney General's Petition should be denied because the materials and information called for in the Contested Requests are protected from disclosure by the attorney-client privilege. See Facebook's Opp. at 22 (arguing that Attorney General's petition seeking "all" internal communications about apps investigated in ADI includes communications that "either involve counsel or were taken at the direction of counsel" and "fall within the heart of attorney-client privilege"). Again, the Attorney General demurs.

"The general features of the attorney-client privilege are well known: the attorney-client privilege shields from the view of third parties all confidential communications between a client and its attorney undertaken for the purpose of obtaining legal advice." *Suffolk Constr. Co. v. Division of Capital Asset Mgt.*, 449 Mass. 444, 448 (2007) ("*Suffolk Constr.*"). See also *Comcast*, 453 Mass. at 303 (recounting the classic formulation of attorney-client privilege: "(1) [w]here legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived") (citation omitted). See also Mass. G. Evid. § 502 (2019). A core policy underlying the attorney-client privilege is to "promote[] candid communications between attorneys and organizational clients." *Chambers v. Gold Medal Bakery, Inc.*, 464 Mass. 383, 395 (2013). See also *Suffolk Constr.*, 449 Mass. at 449 (observing that "[o]ne obvious role served by the attorney-client privilege is to enable clients to make full disclosure to legal counsel of all relevant facts, no matter

how embarrassing or damaging these facts might be, so that counsel may render fully informed legal advice"). "The existence of the privilege and the applicability of any exception to the privilege is a question of fact for the judge," and the "burden of proving that the attorney-client privilege applies to a communication rests on the party asserting the privilege." *Matter of the Reorganization of Elec. Mut. Liab. Ins. Co. Ltd. (Bermuda)*, 425 Mass. 419, 421 (1997).

Here, however, Facebook has not met its burden of proving that *all* internal communications generated in the course of the ADI fall within the scope of the attorney-client privilege. For example, the attorney-client privilege does not extend to any underlying facts or other information learned by Facebook during the ADI, including the identity of the specific apps, groups of apps, and app developers that have been subjected to a "detailed background check" or "technical review" by the Company. See *Upjohn Co. v. United States*, 449 U.S. 383, 395 (1981) ("*Upjohn*") (recognizing that attorney-client privilege "only protects disclosure of communications; it does not protect disclosure of the underlying facts by those who communicated with the attorney"). Facebook cannot conceal such facts from the Attorney General simply by sharing them with its attorneys. *Id.*

Facebook's broad assertion of the attorney-client privilege with respect to the inner-workings of the ADI also is at odds with how the Company has portrayed the ADI publicly. From the very start in March 2018, Facebook has touted the ADI as an investigation and enforcement program undertaken for the benefit of the Company's users, and it has pledged to share information of suspected data misuse uncovered in the course of the ADI with its user community. See Petition, Exhibit GG at 2. Since March 2018, Facebook has provided periodic "updates" to the public about the progress of the ADI, including information about the number of apps purportedly investigated ("millions"), the number of apps that have been suspended ("tens of thousands"), and the number of app developers whose apps have been suspended ("about 400"). See September 2019 Facebook ADI Update at 2. According to Facebook, its goal in doing these things is to,

> bring problems to light so we can address them quickly, stay ahead of bad actors and make sure that people can continue to enjoy engaging in social experiences on Facebook while knowing their data will remain safe.

Id. at 3.

The SJC previously held in comparable circumstances that a private preparatory school could not rely upon the attorney-client privilege to shield from the Commonwealth documents about the school's internal investigation into alleged student-on-student

sexual abuse where the school had "touted its internal investigation to the public in an effort to explain and defend its actions." *Matter of a Grand Jury Investigation*, 437 Mass. 340, 354 (2002). In explaining its reasoning, the SJC observed that the "[t]he school had every right to do this," but further stated that the school could not,

> rely on an internal investigation to assert the propriety of its actions to third parties and simultaneously expect to be able to block third parties from testing whether its representations about the internal investigation are accurate.

Id., citing *United States v. Massachusetts Inst. of Tech.*, 129 F.3d 681, 685-686 (1st Cir. 1997) (acknowledging that disclosure to third party normally negates attorney-client privilege).

Having considered the circumstances and all of the evidence presented by the parties, the Court finds that the materials and information called for in Contested Requests 1 through 5, *supra*, of the Attorney General's Third CID are not protected from disclosure by the attorney-client privilege because they are factual in nature, see *Upjohn*, 449 U.S. at 395, and pertain to the results of an internal investigation that Facebook has affirmatively "touted ... to the public in an effort to explain and defend its actions," see *Matter of a Grand Jury Investigation*, 437 Mass. at 354.

The Attorney General acknowledged at the November 7, 2019, motion hearing, however, that at least some of the "internal communications and internal correspondence" broadly called for in Contested Request 6, *supra*, may very well include requests for legal advice and/or legal advice on the part of Facebook and its attorneys that are classically protected from disclosure by the attorney-client privilege. See, e.g., *Suffolk Constr.*, 449 Mass. at 448. It is not the Court's intention to order the production of such privileged communications and correspondence based on the current record. The duty will fall on Facebook to prepare and provide the Attorney General's Office with a detailed privilege log identifying any allegedly privileged "internal communications and internal correspondence" responsive to Contested Request 6 that are being withheld. The Attorney General then will have the opportunity to review Facebook's privilege log and to challenge, on a case-by-case basis, the Company's decision to withhold specific, individual documents.

Order

For the foregoing reasons, the Attorney General's Petition to Compel Compliance with Civil Investigative Demand Pursuant to G.L. c. 93A, §7 (Docket Entry No. 1) is **ALLOWED IN PART**.

IT IS HEREBY ORDERED THAT, within ninety (90) days of the date of this Decision and Order, Facebook shall:

1. produce to the Attorney General all documents and things in its possession, custody, or control that are reasonably responsive to Contested Requests 1 through 5, *supra*;

2. produce to the Attorney General all non-privileged documents and things in its possession, custody, or control that are reasonably responsive to Contested Request 6, *supra*; and

3. to the extent that it chooses to withhold from its production to the Attorney General on attorney-client privilege grounds any documents or things that are reasonably responsive to Contested Request 6, *supra*, produce to the Attorney General a written privilege log identifying each document withheld and the basis for the assertion of the privilege with sufficient factual detail so as to allow the Attorney General to understand and challenge, if she wishes, Facebook's claim of privilege.

IT IS FURTHER ORDERED THAT the parties shall appear for a status conference before Judge Brian A. Davis in Plymouth Superior Court, 52 Obery Street, Plymouth, Massachusetts, on **March 31, 2020**, at 2:00 p.m.

Brian A. Davis
Associate Justice of the Superior Court

Date: January 16, 2020

Part I ADMINISTRATION OF THE GOVERNMENT

Title XV REGULATION OF TRADE

Chapter 93A REGULATION OF BUSINESS PRACTICES FOR CONSUMERS PROTECTION

Section 6 EXAMINATION OF BOOKS AND RECORDS; ATTENDANCE OF PERSONS; NOTICE

Section 6. (1) The attorney general, whenever he believes a person has engaged in or is engaging in any method, act or practice declared to be unlawful by this chapter, may conduct an investigation to ascertain whether in fact such person has engaged in or is engaging in such method, act or practice. In conducting such investigation he may (a) take testimony under oath concerning such alleged unlawful method, act or practice; (b) examine or cause to be examined any documentary material of whatever nature relevant to such alleged unlawful method, act or practice; and (c) require attendance during such examination of documentary material of any person having knowledge of the documentary material and take testimony under oath or acknowledgment in respect of any such documentary material. Such testimony and examination shall take place in the county where such person resides or has a place of business or, if the parties consent or such person is a nonresident or has no place of business within the commonwealth, in Suffolk county.

(2) Notice of the time, place and cause of such taking of testimony, examination or attendance shall be given by the attorney general at least ten days prior to the date of such taking of testimony or examination.

(3) Service of any such notice may be made by (a) delivering a duly executed copy thereof to the person to be served or to a partner or to any officer or agent authorized by appointment or by law to receive service of process on behalf of such person; (b) delivering a duly executed copy thereof to the principal place of business in the commonwealth of the person to be served; or (c) mailing by registered or certified mail a duly executed copy thereof addressed to the person to be served at the principal place of business in the commonwealth or, if said person has no place of business in the commonwealth, to his principal office or place of business.

(4) Each such notice shall (a) state the time and place for the taking of testimony or the examination and the name and address of each person to be examined, if known, and, if the name is not known, a general description sufficient to identify him or the particular class or group to which he belongs; (b) state the statute and section thereof, the alleged violation of which is under investigation and the general subject matter of the investigation; (c) describe the class or classes of documentary material to be produced thereunder with reasonable specificity, so as fairly to indicate the material demanded; (d) prescribe a return date within which the documentary material is to be produced; and (e) identify the members of the attorney general's staff to whom such documentary material is to be made available for inspection and copying.

(5) No such notice shall contain any requirement which would be unreasonable or improper if contained in a subpoena duces tecum issued by a court of the commonwealth; or require the disclosure of any documentary material which would be privileged, or which for any other reason would not be required by a subpoena duces tecum issued by a court of the commonwealth.

(6) Any documentary material or other information produced by any person pursuant to this section shall not, unless otherwise ordered by a court of the commonwealth for good cause shown, be disclosed to any person other than the authorized agent or representative of the attorney general, unless with the consent of the person producing the same; provided, however, that such material or information may be disclosed by the attorney general in court pleadings or other papers filed in court.

(7) At any time prior to the date specified in the notice, or within twenty-one days after the notice has been served, whichever period is shorter, the court may, upon motion for good cause shown, extend such reporting date or modify or set aside such demand or grant a protective order in accordance with the standards set forth in Rule 26(c) of the Massachusetts Rules of Civil Procedure. The motion may be filed in the superior court of the county in which the person served resides or has his usual place of business, or in Suffolk county. This section shall not be applicable to any criminal proceeding nor shall information obtained under the authority of this section be admissible in evidence in any criminal prosecution for substantially identical transactions.

Part I ADMINISTRATION OF THE GOVERNMENT

Title XV REGULATION OF TRADE

Chapter 93A REGULATION OF BUSINESS PRACTICES FOR CONSUMERS PROTECTION

Section 7 FAILURE TO APPEAR OR TO COMPLY WITH NOTICE

Section 7. A person upon whom a notice is served pursuant to the provisions of section six shall comply with the terms thereof unless otherwise provided by the order of a court of the commonwealth. Any person who fails to appear, or with intent to avoid, evade, or prevent compliance, in whole or in part, with any civil investigation under this chapter, removes from any place, conceals, withholds, or destroys, mutilates, alters, or by any other means falsifies any documentary material in the possession, custody or control of any person subject to any such notice, or knowingly conceals any relevant information, shall be assessed a civil penalty of not more than five thousand dollars.

The attorney general may file in the superior court of the county in which such person resides or has his principal place of business, or of Suffolk county if such person is a nonresident or has no principal place of business in the commonwealth, and serve upon such person, in the same manner as provided in section six, a petition for an order of such court for

the enforcement of this section and section six. Any disobedience of any final order entered under this section by any court shall be punished as a contempt thereof.

Rule 25(a)(1) allows a dismissal of the action upon notice and hearing if the motion for substitution is not timely made, unless the failure of the surviving party to make the motion was the result of excusable neglect. Failure on the part of the decedent's representative to notify the surviving party within a reasonable time from the approval of the bond and to file a suggestion of death upon the record requires a finding of excusable neglect.

Rule 25(b) does not alter prior practice. Neither does Rule 25(c). See Henri Peladeau Lte. v. Fred Gillespie Lumber Co., 285 Mass. 10, 13-14, 188 N.E. 380, 381-382 (1933); Shapiro v. McCarthy, 279 Mass. 425, 428, 181 N.E. 842, 843 (1932).

Rule 25(d) changes prior practice slightly by allowing substitution of a successor officer in place of the officer against whom the action was originally brought. See Knights v. Treasurer & Receiver General, 236 Mass. 336, 341, 342, 128 N.E. 637, 639 (1920).

Rule 26: General Provisions Governing Discovery

(a) Discovery Methods. Parties may obtain discovery by one or more of the following methods except as otherwise provided in Rule 30(a) and Rule 30A(a) , (b) : depositions upon oral examination or written questions; written interrogatories; production of documents or things or permission to enter upon land or other property, for inspection and other purposes; physical and mental examinations; and requests for admission. Unless the court orders otherwise, or unless otherwise provided in these rules, the frequency of use of these methods is not limited.

(b) Scope of Discovery. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

(1) In General. Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party, including the existence, description, nature, custody, condition and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. It is not ground for objection that the information sought will be inadmissible at the trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence.

(2) Insurance Agreements. A party may obtain discovery of the existence and contents of any insurance agreement under which any person carrying on an insurance business may be liable to satisfy part or all of a judgment which may be entered in the action or to indemnify or reimburse for payments made to satisfy the judgment. Information concerning the insurance agreement is not by reason of disclosure admissible in evidence at trial. For purposes of this

paragraph, an application for insurance shall not be treated as part of an insurance agreement.

(3) Trial Preparation: Materials. Subject to the provisions of subdivision (b)(4) of this rule, a party may obtain discovery of documents and tangible things otherwise discoverable under subdivision (b)(1) of this rule and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative (including his attorney, consultant, surety, indemnitor, insurer, or agent) only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of his case and that he is unable without undue hardship to obtain the substantial equivalent of the materials by other means. In ordering discovery of such materials when the required showing has been made, the court shall protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation.

A party may obtain without the required showing a statement concerning the action or its subject matter previously made by that party. Upon request, a person not a party may obtain without the required showing a statement concerning the action or its subject matter previously made by that person. If the request is refused, the person may move for a court order. The provisions of Rule 37(a)(4) apply to the award of expenses incurred in relation to the motion. For purposes of this paragraph, a statement previously made is (A) a written statement signed or otherwise adopted or approved by the person making it, or (B) a stenographic, mechanical, electrical, or other recording, or a transcription thereof, which is a substantially verbatim recital of an oral statement by the person making it and contemporaneously recorded.

(4) Trial Preparation: Experts. Discovery of facts known and opinions held by experts, otherwise discoverable under the provisions of subdivision (b)(1) of this rule and acquired or developed in anticipation of litigation or for trial, may be obtained only as follows:

(A)(i) A party may through interrogatories require any other party to identify each person whom the other party expects to call as an expert witness at trial, to state the subject matter on which the expert is expected to testify, and to state the substance of the facts and opinions to which the expert is expected to testify and a summary of the grounds for each opinion. (ii) Upon motion, the court may order further discovery by other means, subject to such restrictions as to scope and such provisions, pursuant to subdivision (b)(4)(C) of this rule, concerning fees and expenses as the court may deem appropriate.

(B) A party may discover facts known or opinions held by an expert who has been retained or specially employed by another party in anticipation of litigation or preparation for trial

and who is not expected to be called as a witness at trial, only as provided in Rule 35(b) or upon a showing of exceptional circumstances under which it is impracticable for the party seeking discovery to obtain facts or opinions on the same subject by other means.

(C) Unless manifest injustice would result, (i) the court shall require that the party seeking discovery pay the expert a reasonable fee for time spent in responding to discovery under subdivisions (b)(4)(A)(ii) and (b)(4)(B) of this rule; and (ii) with respect to discovery obtained under subdivision (b)(4)(A)(ii) of this rule the court may require, and with respect to discovery obtained under subdivision (b)(4)(B) of this rule the court shall require, the party seeking discovery to pay the other party a fair portion of the fees and expenses reasonably incurred by the latter party in obtaining facts and opinions from the expert.

(5) Claims of Privilege or Protection of Trial Preparation Materials

(A) Information Withheld. When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation material, the party must:

(i) expressly make the claim; and

(ii) describe the nature of the documents, communications, or tangible things not produced or disclosed - and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim. The court, upon motion, may order the withholding party to provide such additional information as is necessary to assess the claim of privilege.

(B) Information mistakenly produced; claim of privilege. If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party shall promptly return, sequester, or destroy the specified information and any copies it has; shall not use or disclose the information until the claim is resolved; shall take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under Trial Court Rule VIII, Uniform Rules on Impoundment Procedure , for a determination of the claim. The producing party shall preserve the information until the claim is resolved.

In resolving any such claim, the court should determine whether:

(i) the disclosure was inadvertent;

(ii) the holder of the privilege or protection took reasonable steps to prevent disclosure; and

(iii) the holder promptly took reasonable steps to rectify the error

(C) Effect of a ruling. If the court, following such procedure, or pursuant to an order under Rule 26(f)(3), upholds the privilege or protection in a written order, the disclosure shall not be deemed a waiver in the matter before the court or in any other proceeding.

(c) Protective Orders. Upon motion by a party or by the person from whom discovery is sought, and for good cause shown, the court in which the action is pending or alternatively, on matters relating to a deposition, the court in the county or judicial district, as the case may be, where the deposition is to be taken may make any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following: (1) that the discovery not be had; (2) that the discovery may be had only on specified terms and conditions, including a designation of the time, place, or manner; or the sharing of costs; (3) that the discovery may be had only by a method of discovery other than that selected by the party seeking discovery; (4) that certain matters not be inquired into, or that the scope of the discovery be limited to certain matters; (5) that discovery be conducted with no one present except persons designated by the court; (6) that a deposition after being sealed be opened only by order of the court; (7) that a trade secret or other confidential research, development, or commercial information not be disclosed or be disclosed only in a designated way; (8) that the parties simultaneously file specified documents or information enclosed in sealed envelopes to be opened as directed by the court.

Factors bearing on the decision whether discovery imposes an undue burden or expense may include the following:

(1) whether it is possible to obtain the information from some other source that is more convenient or less burdensome or expensive;

(2) whether the discovery sought is unreasonably cumulative or duplicative; and

(3) whether the likely burden or expense of the proposed discovery outweighs the likely benefit of its receipt, taking into account the parties' relative access to the information, the amount in controversy, the resources of the parties, the importance of the issues, and the importance of the requested discovery in resolving the issues.

If the motion for a protective order is denied in whole or in part, the court may, on such terms and conditions as are just, order that any party or person provide or permit discovery. The provisions of Rule 37(a)(4) apply to the award of expenses incurred in relation to the motion.

(d) Sequence and Timing of Discovery. Unless the court upon motion, for the convenience of parties and witnesses and in the interests of justice, orders otherwise, methods of discovery may be used in any sequence and the fact that a party is conducting discovery, whether by deposition or otherwise, shall not operate to delay any other party's discovery.

(e) Supplementation of Responses. A party who has responded to a request for discovery with a response that was complete when made is under no duty to supplement his response to include information thereafter acquired, except as follows:

(1) A party is under a duty seasonably to supplement his response with respect to any question directly addressed to (A) the identity and location of persons having knowledge of discoverable matters, and (B) the identity of each person expected to be called as an expert witness at trial, the subject matter on which he is expected to testify, and the substance of his testimony.

(2) A party is under a duty seasonably to amend a prior response if he obtains information upon the basis of which (A) he knows that the response was incorrect when made, or (B) he knows that the response though correct when made is no longer true and the circumstances are such that a failure to amend the response is in substance a knowing concealment.

(3) A duty to supplement responses may be imposed by order of the court, agreement of the parties, or at any time prior to trial through new requests for supplementation of prior responses.

(f) Electronically Stored Information.

(1) Definition.

"Inaccessible electronically stored information" means electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.

(2) Electronically Stored Information Conferences.

(A) Conference as of right. Upon the written request of any party made no later than 90 days after the service of the first responsive pleading by any defendant, the parties shall confer regarding electronically stored information. Such request shall be served on each party that has appeared, but it shall not be filed with the court. The conference shall be held as soon as practicable but no later than 30 days from the date of service of the request.

(B) Conference by agreement of the parties. At any time more than 90 days after the service of the first responsive pleading, any party may serve on each party that has appeared a request that all parties confer regarding electronically stored information. Such request shall not be filed with the court. If within 30 days after the request all parties do not agree to confer, any party may move that the court conduct a conference pursuant to Rule 16 regarding electronically stored information.

(C) Purpose of electronically stored information conference among the parties. The purpose of an electronically stored information conference is for the parties to develop a plan relating to the discovery of electronically stored information. Within 14 days after such conference the parties shall file with the court the plan and a statement concerning any issues upon which the parties cannot agree. At any electronically stored information conference the parties shall discuss:

(i) any issues relating to preservation of discoverable information;

(ii) the form in which each type of the information will be produced;

(iii) what metadata, if any, shall be produced;

(iv) the time within which the information will be produced;

(v) the method for asserting or preserving claims of privilege or of protection of trial preparation materials, including whether such claims may be asserted after production;

(vi) the method for asserting or preserving confidential and proprietary status of information either of a party or a person not a party to the proceeding;

(vii) whether allocation among the parties of the expense of production is appropriate, and,

(viii) any other issue related to the discovery of electronically stored information.

(3) Electronically Stored Information Orders. The court may enter an order governing the discovery of electronically stored information pursuant to any plan referred to in subparagraph (2)(C), or following a Rule 16 conference, or upon motion of a party or stipulation of the parties, or sua sponte, after notice to the parties. Any such order may address:

(A) whether discovery of the information is reasonably likely to be sought in the proceeding;

(B) preservation of the information;

(C) the form in which each type of the information is to be produced;

(D) what metadata, if any, shall be produced;

(E) the time within which the information is to be produced;

(F) the permissible scope of discovery of the information;

(G) the method for asserting or preserving claims of privilege or of protection of the information as trial-preparation material after production;

(H) the method for asserting or preserving confidentiality and the proprietary status of information relating to a party or a person not a party to the proceeding;

(I) allocation of the expense of production; and

(J) any other issue relating to the discovery of the information.

(4) Limitations on Electronically Stored Information Discovery.

(A) A party may object to the discovery of inaccessible electronically stored information, and any such objection shall specify the reason that such discovery is inaccessible.

(B) On motion to compel or for a protective order relating to the discovery of electronically stored information, a party claiming inaccessibility bears the burden of showing inaccessibility.

(C) The court may order discovery of inaccessible electronically stored information if the party requesting discovery shows that the likely benefit of its receipt outweighs the likely burden of its production, taking into account the amount in controversy, the resources of the parties, the importance of the issues, and the importance of the requested discovery in resolving the issues.

(D) The court may set conditions for the discovery of inaccessible electronically stored information, including allocation of the expense of discovery.

(E) The court may limit the frequency or extent of electronically stored information discovery, even from an accessible source, in the interests of justice. Factors bearing on this decision include the following:

(i) whether it is possible to obtain the information from some other source that is more convenient or less burdensome or expensive;

(ii) whether the discovery sought is unreasonably cumulative or duplicative;

(iii) whether the party seeking discovery has had ample opportunity by discovery in the proceeding to obtain the information sought; or

(iv) whether the likely burden or expense of the proposed discovery outweighs the likely benefit.

Amended December 16, 1980, effective January 1, 1981; amended effective July 1, 1996; amended February 27, 2008, effective April 1, 2008; amended September 24, 2013, effective January 1, 2014; amended May 31, 2016, effective July 1, 2016; amended July 11, 2017, effective September 1, 2017.

Reporter's Notes

(2017) The 2017 amendment to Rule 26(b)(5)(A) changed the procedure involving assertions of a claim of privilege or protection of trial preparation materials in connection with discovery requests. It deleted the language that a privilege log must contain specified information--author, recipient, date and type of document, etc.--where a party responding to discovery claimed privilege or protection from discovery.

In 2008, an amendment to Rule 26(b)(5) added the requirement of a privilege log to the Massachusetts discovery rules. The procedure adopted required a designation of each item withheld, document-by-document. Where information was withheld from discovery on the basis that it was privileged or otherwise subject to protection, the withholding party was required to produce a privilege log, unless the parties agreed otherwise in writing. The privilege log was required to list the author and sender (if different) of the document, the recipient, the date and type of document, and the subject matter of the withheld information. In many instances, the requirement of a privilege log listing each document with the required information has proven to be burdensome and in some instances, impractical, given the large number of matters that may exist in an electronic format. This may be especially true where discovery seeks production of electronic mail, text messages, or other forms of electronic communication. Hence, a decision was made to revisit the process.

The 2017 amendment to Rule 26(b)(5)(A) eliminated the requirement of producing a document-by-document log in the first instance containing the specified information. In its place, it adopted an approach used under the Federal Rules of Civil Procedure since 1993. It requires a party seeking to claim privilege or protection to "expressly make the claim" and to "describe the nature of the documents, communications, or tangible things not produced or disclosed…in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim."

CERTIFICATE OF COMPLIANCE

I, Jared Rinehimer , hereby certify that the foregoing brief complies with all of the rules of court that pertain to the filing of briefs, including, but not limited to, the requirements imposed by Rules 16, 20, and 21 of the Massachusetts Rules of Appellate Procedure. The brief complies with the applicable length limit in Rule 20 because it contains 10991 words in 14-point Times New Roman font (not including the portions of the brief excluded under Rule 20), as counted in Microsoft Word (version: Word for Office 365 ProPlus, Version 2002).

/s/ Jared Rinehimer
Jared Rinehimer
Assistant Attorney General

CERTIFICATE OF SERVICE

I hereby certify that on September 30, 2020, I filed with the Supreme Judicial Court and served the attached Brief of the Appellee in *Attorney General* v. *Facebook, Inc.*, No. SJC-12946, by electronic filing and electronic mail upon the following counsel of record:

Felicia H. Ellsworth, Esq.
Rachel L. Gargiulo, Esq.
Eric L. Hawkins, Esq.
Ivan Panchenko, Esq.
Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, MA 02109

Alexander H. Southwell, Esq.
(admitted *pro hac vice*)
Amanda M. Aycock, Esq.
(admitted *pro hac vice*)
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166

Anjan Sahni, Esq.
(admitted *pro hac vice*)
Wilmer Cutler Pickering Hale and Dorr LLP
250 Greenwich Street
New York, NY 10007

/s/ Jared Rinehimer
Jared Rinehimer
Assistant Attorney General
One Ashburton Place
Boston, MA 02108

(617) 963-2594
jared.rinehimer@mass.gov