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