No. DAR-_____
Appeals Court Case No. 2020-P-0456

COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

ATTORNEY GENERAL,

Petitioner-Appellee,

v.

FACEBOOK, INC.,

Respondent-Appellant.

On Appeal from a Decision of the
Superior Court for Suffolk County

APPLICATION FOR LEAVE TO OBTAIN DIRECT APPELLATE REVIEW

FELICIA H. ELLSWORTH (BBO # 665232)
RACHEL L. GARGIULO (BBO # 690747)
ERIC L. HAWKINS (BBO # 693289)
IVAN PANCHENKO (BBO # 693552)
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Felicia.Ellsworth@wilmerhale.com
Rachel.Gargiulo@wilmerhale.com
Eric.Hawkins@wilmerhale.com
Ivan.Panchenko@wilmerhale.com

Attorneys for Respondent-Appellant Facebook, Inc.

April 15, 2020

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21, Respondent-Appellant Facebook, Inc. ("Facebook") states that it has no parent corporation and that there is no publicly held corporation that owns 10 percent or more of the stock of Facebook.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND RULES

INTRODUCTION AND REQUEST FOR DIRECT APPELLATE REVIEW

This case presents fundamental questions about the application of the attorney-client privilege and work product doctrine in the context of attorney-directed internal investigations routinely conducted by companies in the Commonwealth. The case arises from Facebook's ongoing legal response to the 2018 Cambridge Analytica incident—a legal response in which Facebook engaged outside counsel to design and conduct an attorney-led investigation to identify and respond to incidents of data misuse, violations of its privacy policies, and breaches of its contractual terms of service—designed to provide confidential legal advice to the company and to prepare for litigation and regulatory investigations. The decision below compels Facebook to produce information generated by its attorneys during this internal investigation, a decision that upends settled law and warrants this Court's direct review.

This Court has long held that the attorney-client privilege is "a fundamental component of the administration of justice. Today, its social utility is virtually unchallenged." *Suffolk Constr. Co. v. Division of Capital Asset Mgmt.*, 449 Mass. 444, 446 (2007). The privilege "promote[s] broader public interests in the observance of law and administration of justice," *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981), and is "so highly valued" and integral to the "social good" that it outweighs even investigative interests. *Commissioner of Revenue v.*

Comcast Corp., 453 Mass. 293, 304 (2009). Similarly, this Court has made clear that the work product doctrine "enhance[s] the vitality of an adversary system of litigation." *Id.* at 311. And, this Court has recognized that these protections are equally, if not more, important in the context of attorney-led internal investigations. *See, e.g.*, *In re Grand Jury Investigation*, 437 Mass. 340, 351 (2002) ("A construction of the attorney-client privilege that would leave internal investigations wide open to third-party invasion would effectively penalize an institution for attempting to conform its operations to legal requirements by seeking the advice of knowledgeable and informed counsel.").

The Superior Court's decision calls these well-settled protections into question. The order strips the protections of the attorney-client privilege from an internal investigation if a company has announced the mere existence of that internal investigation to the public. Were this the law, companies would be forced to choose between candor to their customers or complying with disclosure obligations, on the one hand, or receiving confidential legal advice, on the other. The order also incorrectly finds work product protections do not attach to a confidential attorney-led investigation launched in anticipation of litigation if a company also has a routine enforcement program on a similar subject matter. Again, if this were the law, companies would be compelled to choose between enforcing their policies in real time or obtaining confidential advice of counsel

when litigation rears its head. Neither of these holdings finds support in Massachusetts law. This Court's review is warranted to clarify the uncertainties introduced by the Superior Court's reasoning below and to reaffirm longstanding protections on which companies doing business in the Commonwealth rely.

* * *

In March 2018—as a result of news reports that University of Cambridge researcher Dr. Aleksandr Kogan and Cambridge Analytica had misused Facebook user data—Facebook faced several civil lawsuits and investigations launched by state, federal, and international regulatory agencies, and anticipated that additional litigations and investigations would follow.

Facebook immediately recognized the legal risks associated with Cambridge Analytica's misconduct and with the anticipated lawsuits and investigations. It therefore sought legal advice to evaluate these risks and to inform its response to existing and anticipated legal challenges. To that end, Facebook hired outside counsel (Gibson, Dunn & Crutcher LLP) and launched a new internal investigation known as the App Developer Investigation (the "Investigation"). From its inception (and continuing through today), the Investigation has been managed and overseen by Facebook's in-house and outside counsel, and information generated in the Investigation is used by counsel to advise Facebook about legal risks and exposure—including how to respond to specific instances of misconduct, as well

as how to respond to the litigations and regulatory inquiries that continue to unfold. In short, the Investigation, like lawyer-led internal investigations conducted by companies all over the Commonwealth, was formed for the purpose of providing legal advice and because of actual and anticipated litigation.

In January 2020, in an order of breathtaking scope, the Superior Court compelled Facebook to turn over to the Attorney General a large amount of information generated by Facebook's counsel in the Investigation. Specifically, the Superior Court ordered Facebook to produce, in response to the Attorney General's Civil Investigative Demand, both confidential communications made within the Investigation and information about particular third-party applications ("apps") that were identified for additional levels of review within the Investigation according to attorney-generated criteria. In sum, the Superior Court ordered Facebook to lay bare to the Attorney General the inner workings of its attorneys' efforts in the Investigation.

But the law is clear that information generated in such attorney-led internal investigations is privileged and protected from disclosure—if it were not, companies like Facebook would be dissuaded from conducting these investigations at all. Just as no Massachusetts court would allow a plaintiff to avoid normal discovery and instead demand that a defendant produce an index of all documents selected for review by its attorneys when investigating a civil complaint, so too has

this Court long protected the efforts of attorneys retained to investigate potential liabilities at a company. Indeed, Facebook relied on this settled law in designing and undertaking the Investigation. The Superior Court's order disregards this law in a manner inconsistent with this Court's precedent, and thus threatens the nature—and, perhaps, the viability—of internal investigations in the Commonwealth.

The Superior Court's order departs from this Court's precedents in several respects. ***First***, the court's ruling nullifies the privilege protections established by *Upjohn Co. v. United States*, 449 U.S. 383 (1981), and its Massachusetts progeny by concluding that Facebook's generic public statements about the Investigation waived attorney-client privilege over the entirety of the Investigation. Specifically, the Superior Court found that Facebook waived the attorney-client privilege by merely notifying its users about the *existence* of the Investigation. Add. 44-45.[1] The implications of that reasoning are far-reaching and troubling: if statements in a press release disclosing the fact of an internal investigation could give rise to waiver or otherwise undermine the privilege, then public companies could be forced to choose between making public statements of any kind—including those

[1] Cites to "Add." refer to the Addendum attached hereto.

that may be required under the disclosure obligations of the securities laws—or risking wholesale waiver of privilege. That is not the law.

Moreover, the Superior Court further erred in finding that communications and information gathered in the Investigation that are "factual in nature" cannot be privileged. But communications in which a client gathers factual information for purposes of obtaining or providing legal advice are unquestionably privileged, and the uncontested record here establishes that the information the Superior Court compelled Facebook to produce is the precise type of fact-gathering for purposes of legal advice that falls comfortably within *Upjohn*'s protective sweep.

Second, the Superior Court incorrectly concluded that the work product doctrine does not apply to documents, communications, and information generated in connection with the Investigation if Facebook would have conducted some of the Investigation's activities irrespective of litigation. In doing so, the court applied a legal framework this Court jettisoned more than ten years ago. In *Commissioner of Revenue v. Comcast Corp.*, 453 Mass. 293 (2009), this Court made clear that the work product doctrine shields information generated "because of" litigation, and expressly rejected an alternative analysis based on whether litigation was the "primary" motive for generating the information. It did so principally to ensure that work product protections would apply to documents serving multiple purposes. Yet here, the Superior Court revived the "primary"

motive test by finding that the threat of litigation was not Facebook's "primary motive" for conducting the Investigation. Add. 52-53.

Next, the Superior Court concluded that the work product doctrine does not protect the Investigation because Facebook employs unrelated monitoring, compliance, and enforcement mechanisms that were not developed in anticipation of litigation. That conclusion contravenes the law and contradicts the uncontested record, which demonstrates that the Investigation is fundamentally distinct from Facebook's preexisting routine enforcement efforts—not least because the new Investigation is differently-structured, lawyer-driven, legally-focused, retrospective, and finite in duration and scope. The Superior Court did not grapple with these undisputed facts at all, instead relying on Facebook's separate routine monitoring efforts as supposedly demonstrating that the Investigation is business-as-usual. It is not.

These grave misapplications of this Court's precedent warrant this Court's direct review. If the Superior Court's order is allowed to stand, any company doing business in the Commonwealth that is contemplating undertaking an internal investigation no longer can be sure that those investigations will remain protected. The Superior Court's order thus raises "novel questions of law," which are "of such public interest that justice requires a final determination by the full Supreme

Judicial Court." Mass. R. App. P. 11(a)(1), (3). Direct appellate review is warranted.

STATEMENT OF PRIOR PROCEEDINGS

The Attorney General commenced her investigation in March 2018 pursuant to Mass. Gen. Laws. c. 93A. In November 2018, she issued a third civil investigative demand ("CID") to Facebook, directly targeting the Investigation. Facebook has produced more than 16,500 pages of non-privileged material across seven productions in response to the third CID, including (for example) communications with third parties. This litigation relates to four requests contained in the third CID that seek information about the Investigation's internal efforts, specifically information about apps identified by internal, confidential, attorney-generated criteria as part of the Investigation, and all communications about those apps. Immediately upon receipt of the third CID, Facebook alerted the Attorney General to the fact that these requests sought materials wholly covered by the privilege and work product protections.[2]

[2] It is undisputed that Facebook immediately made the Attorney General aware of Facebook's privilege and work product objections to these requests in the third CID and that Facebook and the Attorney General have engaged in productive correspondence concerning Facebook's objections since the third CID was issued. Indeed, the Attorney General specifically stated to Facebook in the course of communications about the third CID that she was not asking Facebook to waive privilege or work product.

After extensive correspondence and multiple meet-and-confers about these four requests in the third CID, on August 15, 2019, the Attorney General filed a Petition to Compel Compliance pursuant to Mass. Gen. Laws c. 93A, § 7. The Superior Court granted the Petition on January 16, 2020. Facebook timely noticed its appeal on February 4, 2020. Facebook's appeal was docketed by the Appeals Court on March 19, 2020.[3]

STATEMENT OF RELEVANT FACTS

The following facts are uncontested in the record.

A. Facebook's Platform

Facebook offers an online social networking service that enables people to connect with their friends, family, and communities. In 2007, Facebook launched the Facebook Platform. The Platform allows third-party app "developers" to integrate certain Facebook technologies into their own apps, subject to and restricted by Facebook's Platform policies. Such policies include prohibitions against selling, licensing, or otherwise monetizing user data from Facebook or transferring data to third parties without a Facebook user's consent.

The Platform is designed to empower users to share their Facebook data with apps and developers so users can experience the Internet through new and

[3] Both the Superior Court and a single justice of the Appeals Court declined to stay the Superior Court's order pending Facebook's appeal.

interesting ways. The Platform has not been static since its 2007 launch; for example, before Facebook made changes to the Platform in 2014, users could share information about their friends to the extent allowed by those friends' privacy settings. As part of the 2014 Platform changes, Facebook placed additional, significant limitations on the amount of data developers could request from Facebook users, limited data that developers could access about users' friends, and gave users more control over what information they shared with apps.

Facebook's Investigation pertains only to apps that had access to user data before the 2014 Platform changes. The Investigation does not bear upon Facebook's ongoing enforcement activities on the current Platform.

B. Cambridge Analytica and the Litigations and Regulatory Inquiries That Resulted

In December 2015, Facebook learned that Dr. Aleksandr Kogan, a Cambridge University researcher, violated Facebook's Platform policies by sharing and selling Facebook user data collected through his app with others, including Cambridge Analytica. Facebook took immediate action—it banned Dr. Kogan's app, and secured certifications from Dr. Kogan and Cambridge Analytica that all Facebook user data that they received had been deleted.

In March 2018, several news organizations reported that the data Dr. Kogan and Cambridge Analytica misappropriated may not, in fact, have been deleted—contrary to Dr. Kogan and Cambridge Analytica's certifications to Facebook.

Add. 60-61 (¶¶ 2-3). A wave of litigations and regulatory investigations immediately followed: Facebook has faced well over 60 litigations since March 2018, including this action. These litigations have included securities class actions, developer suits, derivative actions, books-and-records actions, and consumer-based suits. Add. 76-79. Further, Facebook has been subject to formal inquiries from numerous domestic and international regulators, including Congress, the Federal Trade Commission, numerous state attorneys general, the Office of the Privacy Commissioner of Canada, the United Kingdom Information Commissioner's Office, and other foreign regulatory agencies. Add. 67 (¶ 22); Add. 76-79.

C. Facebook's App Developer Investigation

In response to and because of these actual and anticipated legal challenges, and to ascertain whether other developers had engaged in misconduct similar to Dr. Kogan, Facebook launched a new internal investigation, directed by Facebook's in-house counsel, into apps and developers that, like Dr. Kogan and his app, were active before Facebook's 2014 Platform changes and may have had access to large amounts of user data. Add. 61, ¶ 4. Facebook's in-house counsel hired outside legal counsel at Gibson, Dunn & Crutcher LLP to design and direct the Investigation. Add. 63 (¶¶ 6-11).

The Investigation was intentionally structured as a confidential internal legal review. Its specific purpose is to review apps and developers and assess associated legal risks in order to provide advice to Facebook about litigation, regulatory inquiries, and other legal challenges facing the company resulting from potential data misuse. Add. 63 (¶¶ 6-11).

Together with Facebook's in-house counsel, Gibson Dunn designed, managed, and has overseen all stages of the Investigation. Add. 63 (¶¶ 6-11). For example, Gibson Dunn recruited and retained technical experts and investigators to support the Investigation, including two leading forensic consulting firms with expertise in technology-focused investigations. *Id.* Working with these forensic consulting firms, Gibson Dunn and Facebook's internal counsel developed an investigative framework that reflected counsel's assessment of which types of apps pose the greatest legal risks, how Facebook should prioritize its review of apps in light of these risk assessments, and when Facebook should pursue further action, including litigation or referral to relevant regulators. *Id.* Facebook has also taken measures to ensure that the Investigation and information gleaned from it remains confidential, including by restricting communications about the Investigation to only those involved in the Investigation and similarly restricting access to investigatory documents. *Id.*

The Investigation differs in numerous ways from Facebook's preexisting monitoring, compliance, and enforcement efforts. Add. 62, ¶ 5. Unlike the real-time, business-led mechanisms Facebook uses to monitor compliance on the Platform, the Investigation was designed, and has been overseen since its inception, by outside and in-house counsel as a separate *retrospective* evaluation of potential *past* violations of Facebook's policies, with the core purpose of identifying and assessing *legal* liabilities. The Investigation has a finite beginning and end, in contrast to the ongoing real-time efforts of Facebook's business teams. Based on these and other differences, the Investigation is conducted using processes and methodologies that drastically differ from those Facebook uses to assess compliance with its policies as a part of its routine enforcement efforts—including a three-phase investigatory framework for different levels of attorney review that is fully distinct from routine monitoring practices. Add. 64-68 (¶¶ 12-23).

D. Civil Investigative Demands and Petition

The Attorney General has issued three Civil Investigative Demands in the course of her investigation. Facebook has cooperated with each of them. For example, in response to the first two CIDs, Facebook produced nearly 30,000 documents across more than 17 productions. And in response to the third CID, which targeted the Investigation, Facebook has produced more than 16,500 pages

of non-privileged information across seven productions (such as certain communications with third parties), and has provided the Attorney General non-privileged information about the Investigation over eight in-person and telephonic briefings and ten narrative submissions containing detailed information.

At issue here are four requests from the third CID that the Superior Court grouped into six "Contested Requests."

Contested Requests 1 through 5 bear a critical similarity: each request calls for Facebook to provide to the Attorney General the identity of and various other information about apps selected by Facebook's counsel, according to lawyer-developed search criteria, for increased levels of scrutiny and analysis during the course of the Investigation. Each of Contested Requests 1 through 5 thus requires Facebook to turn over attorney-generated information about counsel's evaluation of various levels of legal risk to Facebook in the midst of ongoing litigations and regulatory inquiries. In essence, the Attorney General has asked Facebook for the equivalent of the list of documents selected for review by its attorneys conducting their investigation—a request that stands in stark contrast to a permissible request to produce documents or information meeting certain criteria specified by the Attorney General, which would not inherently call for privileged or work product information. Add. 69-72 (¶¶ 27-36). All told, Contested Requests 1 through 5 call for Facebook to produce information from the Investigation for more than two

million apps (though inclusion of an app in the Investigation does not necessarily indicate data misuse). Add. 69 (¶ 27).

Contested Request 6 sweeps even more broadly, calling for "all" internal communications about the approximately two million apps responsive to Contested Requests 1 through 5. Add. 72 (¶ 37). Contested Request 6 thus directly calls for communications from and among counsel that arose within a privileged internal investigation conducted by and at the direction of counsel, as well as communications pre-dating the Investigation which can only be identified by means of protected work product.

ISSUES OF LAW RAISED BY THIS APPEAL

Facebook seeks Direct Appellate Review on the following two issues that were properly raised and preserved in the Superior Court:

1. Whether a company can be compelled to produce information and communications generated as a part of an internal investigation that was conducted by and at the direction of counsel for purposes of assessing legal risk and providing legal advice.

2. Whether a company that conducts an attorney-led internal investigation in anticipation of litigation can nonetheless be compelled to provide information developed according to lawyer-developed search criteria for various levels of

scrutiny and analysis during the course of that investigation, simply because that company also employs routine non-legal enforcement of its policies.[4]

ARGUMENT

I. THIS COURT SHOULD REAFFIRM THAT THE ATTORNEY-CLIENT PRIVILEGE PROTECTS ATTORNEY INVESTIGATION DOCUMENTS

The Superior Court's conclusion that communications among the investigative team are not privileged rests on two propositions at odds with Massachusetts law: (i) that a company's generic public statements about the existence of an internal investigation waive attorney-client privilege; and (ii) that communications that are "factual in nature" cannot be privileged. These incorrect

[4] On March 30, 2020, a single justice of the Appeals Court declined to stay the Superior Court's order pending appeal. Before turning to the merits, the single justice referenced a potential waiver by Facebook of all privilege and work product protections because Facebook did not formally move to modify or quash the Civil Investigative Demand under G.L. c. 93A, § 6(7). This suggestion is not only incorrect as a matter of law, but was also not before the single justice, as the Attorney General expressly withdrew any waiver argument before the Superior Court—something of which the single justice was apparently not aware. Add. 162-163, Tr. 83:22-25 (Superior Court: "Waiver – you did make a waiver argument in your papers, are you pressing that?" Assistant Attorney General: "I'm not pressing it[.]"). For this reason, this argument was not briefed to the single justice by either Facebook or the Attorney General, and as the Superior Court correctly noted below (Add. 51 n.3), no Massachusetts authority (including the case cited by the single justice) stands for the radical proposition that a party that promptly engages with the Attorney General in response to a CID and explains in detail the substance of its objections while also producing materials in response to non-objected-to portions, must *also* commence litigation over each objected-to portion as well, or lose all rights to object entirely.

propositions set a dangerous precedent that would upend the settled law of privilege in the Commonwealth.

First, relying on dicta in *In re Grand Jury Investigation*, 437 Mass. 340, 354 (2002), the Superior Court improperly held that Facebook waived or somehow undermined its privilege over investigatory communications by "touting" the Investigation "to the public in an effort to explain or defend its actions." Add. 18 (quoting *In re Grand Jury Investigation*, 437 Mass. at 354). But *In re Grand Jury Investigation* stands only for the proposition that when state law *mandates* disclosure of certain legal conclusions, "[a] quintessential element of the attorney-client privilege—the expectation of confidentiality in the results of the investigation" is absent. *Id.* at 352. That holding is inapplicable here: the uncontested record demonstrates that the expectation of confidentiality was and remains a hallmark of the Investigation, Add. 64 (¶ 10), as the Superior Court acknowledged by finding that the privilege does attach to the Investigation. Add. 58.

Further, the Superior Court's erroneous conclusion that Facebook somehow waived or undermined the privilege by "affirmatively 'tout[ing the Investigation] … to the public in an effort to explain and defend its actions,'" Add. 58 (quoting *In re Grand Jury Investigation*, 437 Mass. at 354), is error. Facebook's public statements did not "tout" anything, but simply notified the public that, as part of

Facebook's response to the Cambridge Analytica events, Facebook was investigating data misuse:

> 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. … We will tell people affected by apps that have misused their data.

Add. 45-46; *see also* Add. 46-47 (updating public about Investigation and providing general outline of its process).

To find that these types of generic public statements constitute a waiver or otherwise undermine the privilege would radically expand the waiver doctrine and drastically contract the scope of attorney-client privilege in the Commonwealth. This Court has previously recognized "at issue" waiver only where a party implicitly waives the attorney-client privilege "by injecting certain types of claims or defenses into a case." *Darius v. City of Bos.*, 433 Mass. 274, 284 (2001); *see id.* at 277-279; *Clair v. Clair*, 464 Mass. 205, 218-221 (2013); *McCarthy v. Slade Assocs., Inc.*, 463 Mass. 181, 191-193 (2012). There is a qualitative difference between (i) offering testimony or a defense to gain an adversarial advantage in a judicial proceeding and (ii) publicly disclosing at a high level of generality the subject matter and status of an attorney-led investigation. The former waives the privilege while the latter does not. *See In re Kellogg Brown & Root, Inc.*, 796 F.3d 137, 146-147 (D.C. Cir. 2015) (defendant did not waive privilege where defendant

"neither directly stated that [its internal] investigation had revealed no wrongdoing nor sought any specific relief because of the results of the investigation"); *In re Keeper of Records*, 348 F.3d 16, 24-25 (1st Cir. 2003) (extrajudicial disclosures not used to gain adversarial advantage cannot cause waiver because, "[w]here a party has not thrust a partial disclosure into ongoing litigation, fairness concerns neither require nor permit massive breaching of the attorney-client privilege").[5]

The implications of the Superior Court's ruling are vast: If a company's statements announcing and generally describing an internal investigation could give rise to a subject-matter waiver of privilege, no public company could communicate with its customers or comply with disclosure obligations under federal and state laws without risking waiver. Moreover, companies would be incented to withhold information from the public out of fear that candor would later compel wholesale disclosure of confidential information, harming companies and consumers alike.

Second, the Superior Court found that certain of the information sought by the CID was "factual in nature" and therefore not privileged. Add. 58. But this Court has long recognized that the attorney-client privilege covers communications

[5] *See also In re Fluor Intercontinental, Inc.*, 2020 WL 1487700, at *3-4 (4th Cir. Mar. 25, 2020); *In re General Motors LLC Ignition Switch Litig.*, 80 F. Supp. 3d 521, 528-529, 534 (S.D.N.Y. 2015).

in which a client provides its lawyer with the facts necessary to render legal advice. *See RFF Family P'ship, LP v. Burns & Levinson, LLP*, 465 Mass. 702, 708 (2013) ("[T]he privilege exists to protect not only the giving of professional advice to those who can act on it but also the giving of information to the lawyer to enable him to give sound and informed advice." (quoting *Upjohn*, 449 U.S. at 390)). This is because "[c]ompliance with the law begins with a frank disclosure of the facts to the attorney." *In re Grand Jury Investigation,* 437 Mass. at 351. Indeed, "[t]he 'first step in the resolution of any legal problem is ascertaining the factual background and sifting through the facts with an eye to the legally relevant.'" *Id.* (quoting *Upjohn,* 449 U.S. at 390-391)). Even "purely factual" exchanges between attorney and client are protected from disclosure when those facts are provided to the attorney at his or her request for the purpose of providing legal advice. *See A.W. Chesterton Co. v. Allstate Ins. Co.*, 2001 WL 170460, at *2 (Mass. Super. Ct. Jan. 22, 2001) (finding "a privilege-holder is not required to disclose purely factual portions" of attorney-client communications which is "an essential part of what the attorney-client privilege protects").

Here, the uncontested record establishes that obtaining and providing legal advice was the entire purpose of the Investigation, and that factual information was sought and conveyed in furtherance of that purpose. Thus, internal communications responsive to the Contested Requests—specifically,

communications by and among members of the Investigation team conveying facts necessary for counsel to weigh the legal risks surrounding the apps reviewed by the Investigation—are protected under the attorney-client privilege. The Superior Court's ruling to the contrary is error.

II. THIS COURT SHOULD CORRECT THE SUPERIOR COURT'S UNDULY NARROW CONSTRUCTION OF THE WORK PRODUCT DOCTRINE

The Superior Court also mistakenly concluded that the work product doctrine does not apply to documents, communications, and information generated in connection with the Investigation because Facebook has preexisting monitoring, compliance, and enforcement mechanisms that were not developed in anticipation of litigation. *See* Add. 55. That conclusion contravenes this Court's guidance in *Comcast*, and rests on several fundamental errors concerning the work product doctrine's scope.

First, while purporting to apply *Comcast*'s test for "anticipation of litigation," the Superior Court in fact revived the exact test that *Comcast* expressly rejected. Specifically, the Superior Court credited the Attorney General's argument that "litigation was not Facebook's *primary motive*" for commencing the Investigation. Add. 52 (emphasis added). But whether the prospect of litigation was Facebook's primary, secondary, or tertiary motive is irrelevant if "the document can be fairly said to have been prepared *because of* the prospect of

litigation." *Comcast*, 453 Mass. at 317 (emphasis in original) (internal quotation marks omitted).

The uncontested record manifestly demonstrates that the Investigation was undertaken "because of" litigation, and that materials generated in the Investigation are therefore subject to the protections of the attorney work product doctrine. The Investigation was born in response to actual and anticipated litigation. *See* Add. 61-62 (¶¶ 4-11). From its inception to the present day, attorneys have defined the Investigation's scope, parameters, and operations. *Id.* And the Investigation's purpose is to advise Facebook of its legal positions and risks. *Id.* As even the Superior Court recognized, Facebook retained Gibson Dunn "to design and direct the [Investigation] 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." Add. 46.

That the Investigation, like any other internal investigation, also might promote good business practices does not change the analysis. Indeed, this Court adopted the "because of" framework in *Comcast* precisely because that standard—unlike the erroneous "primary motive" analysis employed by the Superior Court—ensures that work product protections apply to information that serves multiple purposes. *Comcast*, 453 Mass. at 316 ("[The 'because of'] test is consistent with … the purposes of the work product doctrine," which "suggest strongly that work

product protection should not be denied to a document that analyzes expected litigation merely because it is prepared to assist in a business decision.").[6]

Second, the Superior Court's conclusion that the Investigation is "business as usual" simply because Facebook employs other monitoring, compliance, and enforcement programs *not* conducted in anticipation of litigation, Add. 54, fundamentally misapplies this Court's precedent and contradicts the undisputed record. In *Comcast*, this Court recognized a limited exception to the work product doctrine for materials that would have been prepared "irrespective of the prospect of litigation." 453 Mass. at 318 (internal quotation marks omitted). But that limited exception does not mean any company with routine policy enforcement programs automatically loses work product protections for information generated by lawyer-driven investigations like the Investigation. *See Harris v. Steinberg*, 1997 WL 89164, at *3-4 (Mass. Super. Ct. Feb. 10, 1997) (although hospital had policy of "investigating all patient deaths," work product doctrine shielded a non-routine "investigatory memorandum containing a compilation of information … as well as the impressions and conclusions" that were "prepared at the direction of

[6] *See also Mississippi Pub. Emps.' Ret. Sys. v. Boston Sci. Corp.*, 649 F.3d 5, 31 n.24 (1st Cir. 2011) ("[A]n attorney's work product does not lose protection merely because it is also intended to inform a business decision[.]"); *In re Grand Jury Subpoena (Mark Torf/Torf Envtl. Mgmt.)*, 357 F.3d 900, 909-910 (9th Cir. 2004) (documents with "dual purpose character[] fall within the ambit of the work product doctrine").

[counsel]," because hospital "d[id] not normally prepare [documents like those] upon the death of a patient"). Indeed, other courts have concluded that the work product doctrine shields information generated by even routine mechanisms when that information is prepared "because of" litigation. *See Rhodes v. AIG Domestic Claims, Inc.*, 2006 WL 307911, at *4-5 (Mass. Super. Ct. Jan. 27, 2006) (Gants, J.) (although "the evaluation of the facts by claim investigators and claim agents is … performed in the ordinary line of business and duty," "[o]nce litigation has been threatened or commenced, the factual reports of investigation and the internal reports evaluating the strength of the litigation become work product"); *see also id.* at *4 ("If the corporation wished to protect the documents generated by the internal investigation from disclosure in discovery, it would need to direct its attorney to conduct an internal investigation for the purpose of providing legal advice to the company regarding the accident, and have the internal investigation conducted under the direction of that attorney.").

The undisputed record demonstrates that the Investigation is anything but business as usual. Instead, Facebook initiated the Investigation in response to actual and anticipated litigation in the wake of the Cambridge Analytica incident. *See* Add. 61 (¶ 4); *supra* 16-18. Accordingly, even if the Investigation were merely an extension of Facebook's ordinary efforts (which it is not), all documents, communications, and information pertaining to the Investigation still

were generated "because of" anticipated litigation and other legal risks. In failing to recognize that basic principle, the Superior Court rendered the work product doctrine's protections all but illusory.

REASONS WHY DIRECT APPELLATE REVIEW IS APPROPRIATE

Direct appellate review is warranted for two reasons.

First, this appeal involves "novel questions of law which should be submitted for final determination to the Supreme Judicial Court." Mass. R. App. P. 11(a)(1). To resolve this appeal, the Court must determine, among other things: (1) whether a company can be compelled to turn over information and communications generated in the course of an attorney-led investigation designed for the purpose of assessing legal risk; and (2) whether a company can be compelled to provide information developed according to lawyer-developed search criteria for various levels of scrutiny, simply because that company also employs routine non-legal enforcement efforts. These questions, the implications of which are far-reaching, deserve this Court's immediate attention. With internal investigations increasingly commonplace and complicated, this Court's attention is required to reaffirm that the boundaries of the attorney-client privilege and work product doctrine extend to the investigation in this case and others like it.

Second, the issues on appeal are "of such public interest that justice requires a final determination by the full Supreme Judicial Court." Mass. R. App. P.

11(a)(3). The United States Supreme Court and this Court both have recognized that the attorney-client privilege and the work product doctrine are of significant public importance. *See, e.g.*, *Upjohn*, 449 U.S. at 389, 398 (observing that attorney-client privilege "promote[s] broader public interests," and that "strong public policy underl[ies] the work-product doctrine" (internal quotation marks omitted)); *Comcast*, 453 Mass. at 303, 311 (noting that attorney-client privilege serves an "important societal interest," and that work product doctrine "enhance[s] the vitality of an adversary system of litigation" (internal quotation marks omitted)). It is therefore unsurprising that this Court commonly opts to address cases concerning the scope of those bedrock protections without delay—either by granting direct appellate review or on its own initiative. *See, e.g.*, *Chambers v. Gold Medal Bakery, Inc.*, 464 Mass. 383, 389 (2013) (granting application for direct appellate review); *Comcast*, 453 Mass. at 294 (transferring case on own initiative); *In re Grand Jury Investigation*, 437 Mass. at 342 (transferring case on own initiative).

This is just such a case. The Superior Court's order threatens radically to diminish the scope of the attorney-client privilege and work product doctrine, causing companies to reevaluate how to undertake internal investigations—and, perhaps, whether to do so at all. This Court's immediate review is therefore required.

CONCLUSION

The application for direct appellate review should be granted.

Respectfully submitted,

/s/ Felicia H. Ellsworth

FELICIA H. ELLSWORTH
(BBO # 665232)
RACHEL L. GARGIULO
(BBO #690747)
ERIC L. HAWKINS
(BBO # 693289)
IVAN PANCHENKO
(BBO # 693552)
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Felicia.Ellsworth@wilmerhale.com
Eric.Hawkins@wilmerhale.com
Rachel.Gargiulo@wilmerhale.com
Ivan.Panchenko@wilmerhale.com

ANJAN SAHNI
(admitted *pro hac*)
WILMER CUTLER PICKERING
HALE AND DORR LLP
250 Greenwich Street
New York, NY 10007
(212) 230-8800
Anjan.Sahni@wilmerhale.com

ALEXANDER H. SOUTHWELL
(admitted *pro hac*)
AMANDA M. AYCOCK
(admitted *pro hac*)
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166
(212) 351-4000
asouthwell@gibsondunn.com
aaycock@gibsondunn.com

Attorneys for Respondent-Appellant Facebook, Inc.

April 15, 2020

ADDENDUM

TABLE OF CONTENTS

Page

Skip to main content

1984CV02597 Attorney General's Office vs. Facebook Inc

- Case Type
- Business Litigation
- Case Status
- Open
- File Date
- 08/15/2019
- DCM Track:
- B - Special Track (BLS)
- Initiating Action:
- Actions Involving Business Entities and Government
- Status Date:
- 08/15/2019
- Case Judge:
-
- Next Event:
-

All Information | Party | Event | Docket | Disposition

Party Information

Attorney General's Office
- Plaintiff

Alias

Party Attorney
- Attorney
- Cable, Esq., Sara E
- Bar Code
- 667084
- Address
- Office of the Attorney General
  One Ashburton Place
  Boston, MA 02108
- Phone Number
- (617)963-2827
- Attorney
- Downing, Esq., Peter N
- Bar Code
- 675969
- Address
- Office of the Attorney General
  One Ashburton Place
  Boston, MA 02108
- Phone Number
- (617)963-2014
- Attorney
- Rinehimer, Esq., Jared
- Bar Code
- 684701
- Address
- Office of Attorney General Maura Healey
  One Ashburton Place
  18th Floor
  Boston, MA 02108
- Phone Number
- (617)727-2200

More Party Information

Facebook Inc
- Defendant

Alias

Party Attorney
- Attorney
- Ellsworth, Esq., Felicia H
- Bar Code
- 665232
- Address
- Wilmer Cutler Pickering Hale and Dorr LLP
  60 State St
  Boston, MA 02109
- Phone Number
- (617)526-6687
- Attorney
- Gargiulo, Esq., Rachel Lee
- Bar Code
- 690747
- Address
- WilmerHale LLP
  60 State St
  Boston, MA 02209
- Phone Number
- (617)526-6740
- Attorney
- Hawkins, Esq., Eric Lloyd
- Bar Code
- 693289
- Address
- WilmerHale
  60 State St
  Boston, MA 02109
- Phone Number
- (617)526-6926
- Attorney
- Naderi, Esq., Paloma
- Bar Code
- 696679
- Address
- WilmerHale
  7 World Trade Center
  250 Greenwich Street
  New York, NY 10007
- Phone Number
- (212)295-6509

More Party Information

Events

Date	Session	Location	Type	Event Judge	Result
08/29/2019 02:00 PM	Business Litigation 1	BOS-13th FL, CR 1309 (SC)	Motion Hearing	Davis, Hon. Brian A	Rescheduled
09/12/2019 10:00 AM	Business Litigation 1	BOS-13th FL, CR 1309 (SC)	Motion Hearing	Davis, Hon. Brian A	Held as Scheduled
09/12/2019 02:00 PM	Business Litigation 1	BOS-13th FL, CR 1309 (SC)	Motion Hearing	Davis, Hon. Brian A	Rescheduled
11/07/2019 02:00 PM	Business Litigation 1	BOS-13th FL, CR 1309 (SC)	Motion Hearing		Held as Scheduled

Docket Information

Docket Date	Docket Text	File Ref Nbr.
08/15/2019	Attorney appearance On this date Sara E Cable, Esq. added for Plaintiff Attorney General's Office	
08/15/2019	Attorney appearance On this date Jared Rinehimer, Esq. added for Plaintiff Attorney General's Office	
08/15/2019	Attorney appearance On this date Peter N Downing, Esq. added for Plaintiff Attorney General's Office	
08/15/2019	Civil action cover sheet filed. (N/A)	2
08/16/2019	Attorney appearance On this date Felicia H Ellsworth, Esq. added for Defendant Facebook Inc	
08/16/2019	Attorney appearance On this date Eric Lloyd Hawkins, Esq. added for Defendant Facebook Inc	
08/16/2019	Attorney appearance On this date Paloma Naderi, Esq. added for Defendant Facebook Inc	
08/16/2019	Affidavit of Felicia H Ellsworth in Support of Defendant's Ex Parte Motion	4
08/16/2019	The following form was generated: Notice to Appear Sent On: 08/16/2019 11:24:25	
08/16/2019	General correspondence regarding Notice of Acceptance into Business Litigation Session This case is assigned to BLS 1 (dated 8/16/19) notice in hand 8/16/19	5
08/16/2019	Endorsement on Motion to Impound (#3.0): ALLOWED Pursuant to Trial Court Rule VIII, Rule 3(a), the Court ALLOWS this motion on an ex parte basis due the risk of immediate and irreparable harm to the Respondent if the Petition to Compel Compliance and exhibits are not impounded. The Court further ORDERS that, due to its own schedule, good cause exists to extend the duration of this ex parte impoundment Order to and including August 29, 2019. The court will conduct a hearing to determine whether an impoundment order of longer duration should issue on Aug. 29, 2019 at 2:00pm, pursuant to Rule 7(a) (dated 8/16/19) notice in hand 8/16/19	
08/16/2019	Plaintiff Attorney General's Office's Motion for Enlargement of Page Limits with Statement of Reasons in Support (filed 8/15/19)	6
08/16/2019	Plaintiff Attorney General's Office's Motion for Appointment of Special Process Server Kevin McCarthy (filed 8/15/19)	7
08/21/2019	Endorsement on Motion for enlargement of page limits; with statement of reasons in support; (#6.0): ALLOWED notice sent 8/20/19	
08/21/2019	Endorsement on Motion for appointment of special process server; (#7.0): ALLOWED notice sent 8/20/19	
08/22/2019	Endorsement on Motion to (#8.0): ALLOWED impound declaration pending further hearing on 8/29/19	
08/23/2019	Event Result:: Motion Hearing scheduled on: 08/29/2019 02:00 PM Has been: Rescheduled For the following reason: Joint request of parties Hon. Janet L Sanders, Presiding Staff: Margaret M Buckley, Assistant Clerk Magistrate	
08/23/2019	The following form was generated: Notice to Appear Sent On: 08/23/2019 15:10:52	
08/26/2019	Plaintiff Attorney General's Office, Facebook Inc's Motion to Continue August 29 Hearing, and Proposed Briefing Schedule Regarding Impoundment of Materials Filed with Petition to Compel Compliance with Civil Investigative Demand Pursuant to GLc. 93A sec 7: ALLOWED (dated 8/23/19) notice sent 8/26/19	9

Docket Date	Docket Text	File Ref Nbr.
08/26/2019	ORDER: Order Continuing August 29 Hearing and Setting Briefing Schedule Regarding Impoundment of Materials filed with Petition to Compel Compliance with Civil Investigative Demand Pursuant to GLc. 93A sec 7 (see P#10 for order) (dated 8/23/19) notice sent 8/26/19	10
08/26/2019	ORDER: Allowing impoundment of respondent Facebook's Declaration in support of its Motion for continued impoundment Notice sent 8/23/19 (entered 8/22/19) Judge: Sanders, Hon. Janet L	11
08/26/2019	Affidavit of Felicia H Ellsworth in support Emergency Motion to impound Declaration in support of respondent's Motion for continued impoundment (entered 8/22/19) IMPOUNDED	12
09/04/2019	The following form was generated: Notice to Appear Sent On: 09/04/2019 07:46:39	
09/04/2019	Event Result:: Motion Hearing scheduled on: 09/12/2019 02:00 PM Has been: Rescheduled For the following reason: Request of Defendant Hon. Brian A Davis, Presiding Staff: Margaret M Buckley, Assistant Clerk Magistrate	
09/05/2019	Respondent Facebook Inc's Motion for continued Impoundment	13
09/05/2019	Attorney appearance On this date Rachel Lee Gargiulo, Esq. added for Defendant Facebook Inc	
09/09/2019	Plaintiff Attorney General's Office's Assented to Motion to impound affidavit in support of Petitioner's opposition to respondent's Motion for continue impoundment	14
09/10/2019	Endorsement on Motion to (#14.0): ALLOWED impound affidavit Notice sent 9/11/19	
09/12/2019	Opposition to of the Attorney General to respondent's Motion for continued impoundment filed by Facebook Inc	15
09/12/2019	Event Result:: Motion Hearing scheduled on: 09/12/2019 10:00 AM Has been: Held as Scheduled Hon. Brian A Davis, Presiding Staff: Margaret M Buckley, Assistant Clerk Magistrate	
09/16/2019	ORDER: allowing impoundment of petitioners affidavit in opposition to respondent's motion for continued impoundment Notice Sent 9/11/19	17
09/16/2019	Plaintiff Attorney General's Office, Facebook Inc's Submission of Joint Proposed Briefing Schedule Regarding Petition to Compel Compliance with Civil Investigative Demand Pursuant to GL.c. 93A sec 7 and Request for Hearing: ALLOWD (dated 9/12/19) notice sent 9/12/19	19
09/24/2019	Respondent Facebook Inc's EMERGENCY Motion to enlarge the time for filing Facebook's response to the petition and the Attorney General's reply to the petition ALLOWED (dated 9/25/19). This motion is Allowed. Facebook shall file its response to the Petition on or before Oct. 7, 2019, and the Attorney General shall file her reply on or before Oct. 28, 2019. The Court will hear the petition on Nov. 7, 2019 at 2:00pm. (Davis, J.) Notice sent 9/27/19.	20
09/26/2019	The following form was generated: Notice to Appear Sent On: 09/26/2019 08:19:29	
10/02/2019	Plaintiff Attorney General's Office's Assented to Motion for admission of Anjan Sahni Alexander H Southwell and Amanda M Aycock Pro Hac Vice	21

Docket Date	Docket Text	File Ref Nbr.
10/07/2019	Respondent Facebook Inc's Assented to Motion to enlarge page limit of respondent's opposition to the attorney general's petition (w/opposition)	22
10/09/2019	Endorsement on Motion for admission of Anjan Sahni Alexander H Southwell and Amanda M Aycock Pro Hac Vice (#21.0): ALLOWED (dated 10/7/19) notice sent 10/9/19	
10/15/2019	ORDER: Order on Impoundment The following Materials are hereby IMPOUNDED: (a) Attorney Healey's Petition to Compel Compliance with Civil Investigative Demand; (b) Attorney General's Memo of Law in Support of the Petition; (c) Exhibits I, J, K, L, M, EE, LL, MM, PP, QQ, RR, TT and UU to the Petition; (d) The compact disc filed by Attorney General; (e) The Satterfield Declaration; (f) The Cable Declaration. The Impoundment Order of 8/23/19 is hereby LIFTED as to Exhibits A, B, C, D, E, F, G, H, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, AA, BB, CC, DD, FF, GG, HH, II, JJ, KK, NN, OO and SS to the Petition. The parties have filed a package containing versions of the Attorney General's Petition, Memorandum in Support and Exhibits A through UU (The public Filings). The clerk shall enter the public Filings on the Docket and make them available to the public. Within the Public Filings are the following pleadings and documents that are REDACTED to reflect the impoundment ordered by this court: (a) The Attorney General's Petition to Compel Compliance to Civil Investigative Demand Pursuant to GLc. 93A sec 7; (b) The Attorney General's Memorandum of Law in Support of the Petition, and (c) Exhibits I, LL, MM, PP,QQ, RR, TT, and UU to the Petition. The Public filings also contain replacement Exhibits P, S, V, W, X, Y, Z, AA, BB, and CC. The clerk Shall replace Exhibits P, S, V, W, X, Y, Z, AA, BB, and CC, as they appear in the Attorney General's August 15, 2019 filing with the Replacement Exhibits. SO ORDERED (see P#23 for complete Order) (dated 9/20/19) notice in hand 9/20/19	23
10/15/2019	Original civil complaint filed: REDACTED Petition to Compel Compliance with Civil Investigative Demand Pursuant to GLc. 93A sec 7	24
10/15/2019	Plaintiff Attorney General's Office's Memorandum of Law in Support of the Attorney General's Petition to Compel Compliance with Civil Investigative Demand (REDACTED)	25
10/15/2019	Defendant Facebook Inc's Memorandum in Opposition to the Attorney General's Petition to Compel Compliance with Civil Investigative Demand Pursuant to GLc. 93A sec 7	26
10/15/2019	Docket Note: : Exhibits A, B, C, D, E, F, G, H, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, AA, BB, CC, DD, FF, GG, HH, II, JJ, KK, NN, OO and SS to the Petition placed in the public File; Exhibits P, S, V, W, X, Y, Z, AA, BB and CC are replacement exhibits; Exhibits I, LL, MM, PP, QQ, RR, TT and UU Are REDACTED exhibits.	
10/15/2019	Endorsement on Motion to Enlarge Page Limit of Respondent's Opposition to the Attorney General's Petition (#22.0): ALLOWED /(dated 10/9/19) notice sent 10/11/19	
10/15/2019	Affidavit of Stacy Chen in Support of Respondent's Opposition to the Attorney General's Petition (filed 10/7/19)	29
10/24/2019	Petitioner Attorney General's Office's Assented to Motion for an Enlargement of Page Limit of the Attorney General's Reply to Facebook's Opposition to the Attorney General's Petition	30
10/28/2019	Opposition to to the Petition to compel compliance with Civil Investigative demand filed by Attorney General's Office	31
10/30/2019	Endorsement on Motion for Enlargement of Page Limit (#30.0): ALLOWED up to 15 pages, including signature page (dated 10/28/19) notice sent 10/29/19	
11/07/2019	Event Result:: Motion Hearing scheduled on: 11/07/2019 02:00 PM Has been: Held as Scheduled Hon. Brian A Davis, Presiding Staff: Norman W Huggins, Assistant Clerk Magistrate	
01/21/2020	ORDER: decision and order regarding Attorney General's Petition to compel compliance with civil investigative demand to G.L. c. 93A Sec. 7 (docket entry No. 1.0); ALLOWED in part; (see paper No. 32.0 for full order); (dated 1/16/20) notice sent 1/17/20	32

Docket Date	Docket Text	File Ref Nbr.
02/04/2020	Notice of appeal filed. Notice sent 2/7/20 Applies To: Facebook Inc (Defendant)	33
02/13/2020	Certification/Copy of Letter of transcript ordered from Court Reporter 11/07/2019 02:00 PM Motion Hearing	34
02/13/2020	Transcript of 11/7/19 received	
02/20/2020	Respondent Facebook Inc's Motion to Stay Order Regarding Attorney General's Petition to Compel Compliance Pending Appeal and Memorandum in Support of (Expedited Treatment Requested)	35
02/20/2020	Opposition to Respondent's Motion to Stay Order Regarding Attorney General's Petition to Compel Compliance Pending Appeal filed by Attorney General's Office	36
02/20/2020	Brief filed: Reply Facebook's Reply Brief in Support of its Motion to Stay (Expedited Treatment Requested) Applies To: Facebook Inc (Defendant)	37
03/05/2020	ORDER: regarding respondents motion to stay order regarding Attorney General's petition to compel compliance pending appeal (docket No. 35); motion is DENIED; (see paper No. 38 for full decision and order) (dated 3/2/20) notice sent 3/5/20	38
03/09/2020	Notice of assembly of record sent to Counsel Applies To: Ellsworth, Esq., Felicia H (Attorney) on behalf of Facebook Inc (Defendant); Cable, Esq., Sara E (Attorney) on behalf of Attorney General's Office (Plaintiff); Downing, Esq., Peter N (Attorney) on behalf of Attorney General's Office (Plaintiff); Rinehimer, Esq., Jared (Attorney) on behalf of Attorney General's Office (Plaintiff); Gargiulo, Esq., Rachel Lee (Attorney) on behalf of Facebook Inc (Defendant); Hawkins, Esq., Eric Lloyd (Attorney) on behalf of Facebook Inc (Defendant); Naderi, Esq., Paloma (Attorney) on behalf of Facebook Inc (Defendant)	
03/09/2020	Notice to Clerk of the Appeals Court of Assembly of Record	
03/09/2020	ORDER: regarding respondent's motion to stay order regarding Attorney General's petition to compel compliance pending appeal (docket No. 35); (dated 3/2/20) notice sent 3/9/20	39
03/20/2020	Notice of Entry of appeal received from the Appeals Court In accordance with Massachusetts Rule of Appellate Procedure 10(a)(3), please note that the above-referenced case (2020-P-0456) was entered in this Court on March 19, 2020.	40
03/24/2020	Notice of Entry of appeal received from the Appeals Court On March 19, 2020, the above-referenced case was entered on the docket of the Appeals Court.	41

Case Disposition

Disposition	Date	Case Judge
Pending		

NOTIFY

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

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

29

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
NO. 1984CV02597-BLS-1

ATTORNEY GENERAL
MAURA HEALEY

Petitioner,

v.

FACEBOOK, INC.,

Respondent.

SUFFOLK SUPERIOR COURT
CIVIL CLERK'S OFFICE
2019 OCT -7 P 3:11
RICHARD JOSEPH DONOVAN
CLERK / MAGISTRATE

DECLARATION OF STACY CHEN IN SUPPORT OF RESPONDENT'S OPPOSITION TO THE ATTORNEY GENERAL'S PETITION

I, Stacy Chen, hereby attest to the following facts based on my personal knowledge and on information gathered under my supervision and direction. If sworn as a witness to testify in this matter, I would testify to the facts set forth herein.

1. I am Associate General Counsel at Facebook, Inc., and a member of Facebook's Platform Litigation Enforcement team. I have served in this capacity since April 2018. In this capacity, I have overseen the App Developer Investigation with a core investigative team that I lead at the company. I have worked at Facebook since December 2014.

Background and The App Developer Investigation

2. In November 2013, a Cambridge University researcher named Aleksandr Kogan created a personality app (the "App") on the Facebook Platform. In December 2015, news outlets reported that Dr. Kogan violated Facebook's Platform Policies by sharing and selling data collected through the App with others, including Cambridge Analytica and Christopher Wylie of Eunoia Technologies, Inc. When Facebook learned of this

violation in 2015, Facebook removed the App from Facebook and demanded certifications from Kogan and all parties to whom he had given data that the information had been destroyed. Cambridge Analytica, Kogan, and Wylie all certified that they had destroyed the data.

3. In March 2018, the New York Times and the Guardian of London reported that the data collected and shared by Dr. Kogan in violation of Facebook's policies may not have actually been deleted. These reports triggered extensive media attention surrounding the Cambridge Analytica events and almost immediately triggered litigation and regulatory inquiries, including, for example:

   - legal matters related to apps and developers that, like Dr. Kogan and his App, may have misused information from the time period before Facebook placed additional, significant limitations on the amount and type of data developers could request from users through the Facebook Platform;
   - legal matters involving Facebook and its directors and officers alleging, *inter alia*, violations of the U.S. securities laws and breach of fiduciary duties;
   - legal matters alleging, *inter alia*, violations of consumer protection statutes and common law claims for breach of contract and fraud; and
   - investigations and potential enforcement actions against the company at both the state and federal levels and from international regulators.

4. Facebook anticipated that it would have to respond to known and expected legal challenges in connection with apps and developers that, like Dr. Kogan and his App, may have had access to large amounts of user data because they were active before Facebook placed additional, significant limitations on the amount and type of data developers could

request from users through the Facebook Platform in 2014. Further, light of the nature of the inquiries and matters described above, Facebook determined that an attorney-led investigation was necessary to evaluate the legal risks associated with third-party developer access to and use of data prior to the changes implemented by the company in 2014. From the outset, the company contemplated a review of potentially millions of apps that would inform the company's legal strategy.

5. For context, a legal-led investigation is not Facebook's typical response when the company determines that violations of its Platform policies may have occurred. Rather, the Developer Operations ("DevOps") team, along with the policy team managing Facebook's Platform Policy, have historically been the front lines to address potential violations of Platform policies and subsequent enforcement efforts. Escalations regarding non-cooperative developers could be escalated by legal should a cease and desist letter or more aggressive legal enforcement be warranted. The DevOps team is a team internal to Facebook that operates under the direction of Facebook employees. Unlike in the typical case, however, an attorney-led investigation was necessary here because, though they had investigative personnel, DevOps and the Platform Policy team neither had the capacity nor were they set up to: (i) address the company's legal risks with respect to the historical Platform; (ii) address compliance risks with applicable laws regarding the historical Platform; or (iii) assess Facebook's position in pending or anticipated litigation or regulatory inquiries. Moreover, given the historical focus of the investigation's inquiry, significant investigation was required to develop the framework and baseline data that would form the foundation of the investigation.

6. At Facebook management's request, Facebook's in-house legal team retained outside counsel (Gibson Dunn & Crutcher LLP) experienced with cybersecurity and data privacy internal investigations to design and direct a new investigation that could, among other things, gather the facts necessary for providing legal advice to Facebook about litigation, compliance, regulatory inquiries, and other legal risks facing the company resulting from potential data misuse and activities by third-party app developers operating on the prior version of the Platform. Facebook in-house attorneys including myself, along with a core investigative team including members of the Partnerships, Data Policy, and DevOps teams, collaborated with Gibson Dunn to build out what became more formally known as the "App Developer Investigation," or the "ADI."

7. Unlike Facebook's other enforcement efforts, the ADI is in essence a historical investigation to determine whether there has been misuse of data in violation of Facebook's policies and associated legal liabilities, in connection with the first version of the Platform.

8. From the beginning, Gibson Dunn and Facebook's in-house counsel have designed, managed, and overseen all stages of the ADI, with the input of subject matter experts across the company. The ADI was developed distinctly from the processes and investigative methodologies previously used to assess third parties' compliance with Facebook policies. ADI's mandates include assessing the legal risks to Facebook of data misuse by conducting a legally-driven and scaled lookback analysis of apps that had access to large amounts of user data before the 2014 Platform changes, and providing legal advice to Facebook about litigation, regulatory inquiries, and other legal risks facing the company resulting from potential data misuse from earlier versions of the platform.

There is no industry standard for how to conduct such an investigation. Rather, under Gibson Dunn's and in-house counsel's leadership, the ADI investigative team devised and tailored the ADI's methods, protocols, and strategies to address the specific risks posed by these legal challenges.

9. Gibson Dunn led the recruitment and retention of technical experts and investigators, including two leading forensic consulting firms with expertise in assisting with technology-focused internal investigations, for the ADI. The scope of engagement for each of these consulting firms was to operate as an extension of Facebook counsel and support counsel's provision of legal advice. Together, these teams developed an investigative framework that reflected counsel's assessment of risky app and developer profiles, how Facebook should prioritize its review, and when Facebook should pursue further enforcement action, including litigation.

10. Gibson Dunn and in-house counsel have taken steps to ensure that communications by and among the ADI investigatory team remain confidential and privileged, including by instructing the team to limit communications about ADI and access to investigatory documents to only employees, consultants, and counsel who needed access to them. In addition, materials created in the course of the ADI are stored securely, with access limited to those necessary to the investigation.

11. Gibson Dunn and in-house counsel, with the assistance of the expert investigative consultants, developed a process that involved three investigative phases: (1) Detection and Identification; (2) Enhanced Examination; and (3) Enforcement.

12. Phase One: Detection and Identification. At the direction of Gibson Dunn and in-house counsel, the ADI investigatory team (consisting of the Gibson Dunn team, Facebook

employees, and the forensic consultants retained for ADI), worked to develop, test, and refine methodologies and selection criteria to identify apps posing legal risk that would warrant escalation for further investigation. Based on this information, the team developed four risk-based approaches to conduct the investigation based on an assessment of where and how the greatest legal risk to the company might arise. Identification by one of these methods only meant that an app warranted further inquiry, not necessarily that the app misused data.

13. The first risk-assessment methodology designed by counsel is the **User Impact Method**, in which counsel prioritized individual apps for review based on their having a large number of users, which would suggest a larger user impact should data misuse be found. Importantly, however, this method did not only focus on apps with the largest overall number of users; it also focused on apps with permissions to access a certain volume and type of sensitive data—thresholds which counsel developed with input from internal subject matter experts at Facebook.

14. The second risk-assessment methodology designed by counsel is the **Categorical Method**. This methodology was developed by counsel working with the forensic consultants and internal experts. Through this methodology, categories of apps and developers believed to present elevated risk of potential policy violations (and accordingly, greater legal risks) were developed.

15. The third risk-assessment methodology designed by counsel is the **Escalations Method.** Under this methodology, counsel worked to identify the types of ad-hoc escalations that merited further investigation by the ADI team (as compared with a different Facebook

team), recognizing the legal risk associated with apps flagged throughout the company through various ad hoc methods.

16. The fourth risk-assessment methodology is the **Low-Impact Method.** Counsel, assisted by the forensic consultants, developed a risk-based, data-driven approach to deprioritize apps for review that did not pose as much legal risk as others. This included methodologies for identifying apps that neither obtained access to large amounts of user data nor held sensitive permissions for a significant number of users.

17. Phase Two: Enhanced Examination. Under Enhanced Examination, after an app or developer has been identified for further review based on the criteria outlined above, counsel directs the ADI forensic team to conduct intensive background and technical investigations, and the ADI forensic team reports their findings to counsel. A report for a single developer can include extensive technical and other details and are specifically tailored, in substance and format, for outside counsel to evaluate the potential for data misuse. Some reports may cover a single app; others may cover many apps of a single developer.

18. Enhanced Examination may also include application of a model (called the Risk-Prioritization Formula) developed under the guidance of counsel that assists in assessing the data-access risk based in part on the permissions granted to apps and the number of users that authorized specific permissions. The Risk-Prioritization Formula is used to prioritize apps for review during the Enhanced Examination phase.

19. Phase Three: Enforcement. In the final phase of ADI, outside counsel review the results of these investigations, recommend next steps to Facebook in-house counsel for approval, and draft requests for information or other follow-up sent to developers. If outside

counsel determine that an information request response was inadequate, counsel may attempt various additional engagement with the developer, including conducting interviews or requesting audits of data security or storage infrastructure.

20. At this stage, outside counsel, in consultation with the ADI team and a number of internal Facebook teams, determine on a case-by-case basis if any additional enforcement action is appropriate, such as suspending the developer and/or the app. Outside counsel also make recommendations about whether Facebook should take legal measures, including sending cease and desist letters, or engaging in litigation against developers.

21. A partnership with the outside expert consulting firms and Facebook personnel from various teams that comprise the ADI investigatory team was necessary for Gibson Dunn and in-house counsel to effectively advise Facebook as its legal counsel for a variety of reasons, including to provide compliance advice regarding Facebook's operations, to develop legal strategy for active and anticipated litigation matters and regulatory inquiries, and to evaluate potential legal exposure. The ADI investigatory team works at the direction of counsel, relies on counsel's input and guidance, and has played a pivotal, necessary role in facilitating legal advice by counsel and implementing that advice by the company.

22. Gibson Dunn and in-house counsel structured the ADI in view of its core purpose: to enable counsel to obtain the information needed to provide effective legal advice to Facebook. As the ADI has progressed, Facebook outside and in-house counsel have used information uncovered through it to advise the company on how best to protect Facebook's legal rights and mitigate the company's risks in the face of threatened and pending litigation and regulatory inquiries centering on the misuse of user data by third-

party apps, including in connection with securities class actions, derivative actions, books-and-records actions, consumer class actions, various suits by developers (including from Dr. Kogan, who has sued Facebook in the Southern District of New York, and other actions by developers in the United Kingdom and Italy), and inquiries from numerous domestic and international regulators, including Congress, the Federal Trade Commission, state attorneys general, the Office of the Privacy Commissioner of Canada, the United Kingdom Information Commissioner's Office, and other foreign regulatory agencies.

23. Gibson Dunn and in-house counsel have also used information uncovered through the ADI to develop strategy for and pursue offensive litigation. For example, the ADI investigated whether a South Korean app developer, Rankwave Co., Ltd. ("Rankwave"), used Facebook user data to provide marketing and advertising services in violation of Facebook policies. Following that investigation, on the advice of counsel, Facebook sent Rankwave a request for information ("RFI"). When Rankwave failed to respond to the RFI, Gibson Dunn sent Rankwave a cease-and-desist letter and communicated with Rankwave to get more information about its data practices. Ultimately, when Rankwave refused to cooperate, Facebook filed suit against Rankwave in California. The lawsuit is ongoing.

24. Attached hereto as **Exhibit 1** is a list of all pending domestic and international litigation relating to the Cambridge Analytica events and the misuse of user data by third-party apps as of the date of this declaration. This multitude of threatened and pending litigation was and is the backdrop of the ADI and, as such, has been a significant driving force behind the decisions made by Facebook counsel throughout the ADI process.

Documents and Information Sought by the Petition

25. I have reviewed the categories of documents and information sought by the Attorney General's third CID and Petition.

26. The Petition seeks the Court to order Facebook to "comply in full with requests 1-3 and 6" of the third Civil Investigative Demand ("CID") with respect to the following subsets of apps: (a) approximately 6,000 apps with a large number of installing users; (b) apps that Facebook identified for review based on "past investigative experience"; (c) apps that were reported to Facebook from outside of the ADI process; (d) apps for which Facebook has conducted a detailed background check; and (e) apps for which Facebook has conducted a technical review.

27. **CID Request No. 1.** I understand this Request seek a list of all apps that the ADI team identified in the Detection and Identification (Phase One) aspect of the ADI. As detailed in paragraphs 11 to 15, counsel selected apps for Phase One review via: (i) the User Impact Method; (ii) the Categorical Method; and (iii) the Escalations Method. Construed in conjunction with Petition Prayers for Relief 2(a), 2(b), and 2(c), this Request calls for three separate lists of attorney-selected and compiled apps, which total approximately two million apps.

28. Facebook has not made productions responsive to Request No. 1 because, as Facebook has previously explained to the Attorney General, this Request seeks information prepared at the direction of counsel in furtherance of the ADI and in anticipation of litigation.

29. Prior to identification and compilation by Facebook counsel, the attorney-created lists of apps associated with the User-Impact Method, Escalation Method, Categorical Method

did not exist as raw data that counsel could simply turn over to the Attorney General. Rather, the data compilations identifying the apps at issue in Request No. 1 were prepared at the direction of Facebook counsel pursuant to the ADI and done to assist Facebook counsel with providing legal advice to Facebook, minimizing the company's litigation risk, and preparing for litigation against the company.

30. **CID Request No. 2.** I understand that this Request is seeking detailed information regarding the ADI team's review of the roughly two million apps from Request 1, as well as the following: (a) the app's developer; (b) whether the app is a test app or was released to the public; (c) when the app was first released to the public; (d) the date Facebook first reviewed the app's privacy policy and a description of the nature of that review; (e) the basis for investigation of the app; (f) the app's permissions; (g) the number of users who installed or downloaded the app; and (h) the number of users whose information was accessed or obtained by the app who did not download or install the app.

31. Facebook has not made productions responsive to this request because, as Facebook has previously explained to the Attorney General, much of the information and data sought by Request No. 2 does not exist as business records and, to the extent that responsive information exists as records, it is largely composed of data compilations or selections that were prepared at the direction of counsel in furtherance of the ADI. To the extent that responsive information does not exist, it would require attorney synthesis and generation to create or compile.

32. In particular, prior to compilation by Facebook counsel, the data identifying the apps at issue in Request No. 2(a), and (f)-(g) did not exist as raw data that counsel could turn over to the Attorney General. Rather, each were prepared at the direction of Facebook

counsel pursuant to the ADI and done to assist Facebook counsel with providing legal advice to Facebook about potential risks and active and potential litigation.

33. Facebook does not maintain information responsive to Request No. 2(b)-(e) or (h) in the ordinary course of business. It would be extremely difficult to create a compilation of the information sought by these Requests for the roughly two million apps at issue. More importantly, these Requests ask Facebook to divulge information about counsel's strategy and thought processes in developing the ADI investigative framework, including by providing "a description of the nature" of the ADI's review of the app's privacy policy and the "basis" and "initial source(s)" of concerns of data misuse.

34. **CID Request No. 3.** I understand this Request to seek identification of apps falling into nine separate categories that have been escalated to Phase Two of ADI for Enhanced Examination and/or Phase Three of ADI for Enforcement, including: (a) each app that received an in-depth review; (b) each app for which a Background Information investigation was conducted; (c) each app for which a Technical Investigation was conducted; (d) each app to which a request for information was sent; (e) each app for which an interview was sought with the developer; (f) each app for which a remote or onsite audit was requested to be conducted; (g) each app for which actual misuse was found and identification of that misuse; (h) each app that was banned for actual misuse; and (i) each app that was banned for failing to cooperate with Facebook's investigation. I understand Prayers for Relief 2(d) and 2(e) correspond to CID Requests Nos. 3(b) and 3(c), i.e., applications that have undergone a background investigation or technical review.

35. Six of the nine categories (Requests 3(d)-(i)) call for information which is not privileged, which Facebook has already produced. Facebook has also provided lists of apps that are the subject of external—and thus non-privileged—actions or communications with third parties, including the growing list of applications it has suspended as part of the Investigation, whether because of policy violations or because of their refusal to cooperate with Facebook's investigation. The most recent version of this list, from July 23, 2019, includes nearly 69,000 apps.

36. Of the remaining three categories (Requests 3(a)-(c) of the third CID), the Request seeks the identity of apps that the ADI selected for an "in-depth review," background investigations, and technical investigations. Facebook has not produced this information because it is privileged. Counsel selected each of these groups of apps by developing customized risk-based approaches based on counsel's assessment of where and how the greatest legal risk to the company might arise. The data compilations identifying the apps at issue in Request No. 3(a) – (c) were prepared at the direction of Facebook counsel pursuant to the ADI and done to assist Facebook counsel with providing legal advice to Facebook regarding potential risks and active and potential litigation.

37. **CID Request No. 6.** I understand that this Request seeks *all* internal Facebook and ADI communications related to the apps reviewed in the ADI. The communications and correspondence responsive to Request No. 6 as to the millions of apps at issue are communications between and among Facebook in-house counsel, Gibson Dunn, and internal and outside experts and investigators. Facebook has not made productions of correspondence responsive to this Request because, as Facebook counsel notified the Attorney General on numerous occasions, these communications concerning the ADI

involve counsel acting in their legal capacity or were undertaken by expert consultants or Facebook employees acting at the direction of Facebook counsel, and as an extension of counsel, including for purposes of gathering facts necessary to conduct their legal analysis and to assist them with providing legal advice to Facebook. Facebook has, however, produced to the Attorney General substantial non-privileged ADI-related communications between Facebook and developers.

Executed on this 7th day of October 2019.

Stacy Chen
Associate General Counsel
Facebook, Inc.

2019.
2597
34

CERTIFICATE OF SERVICE

I hereby certify that I will serve a true copy of the foregoing document upon counsel of record as follows:

Maura Healey
Attorney General of the
Commonwealth of Massachusetts

Sara Cable, BBO #667084
Assistant Attorney General
Director, Data Privacy & Security Unit
sara.cable@mass.gov

Jared Rinehimer, BBO #684701
Assistant Attorney General
jared.rinehimer@mass.gov

Peter Downing, BBO #675969
Assistant Attorney General
peter.downing@mass.gov

Consumer Protection Division
Office of Attorney General Maura Healey
One Ashburton Place
Boston, MA 02108
(617) 727-2200

Felicia H. Ellsworth

Dated: October 7, 2019

Exhibit 1

Representative Litigation Relating To Cambridge Analytica Events

No.	Case/Matter Name	Case Number	Date Filed	Jurisdiction[1]
Securities Class Action Litigation				
1.	In re Facebook, Inc. Securities Litigation	No. 5:18-cv-01725-EJD	03/20/2018	Northern District of California
2.	Helms v. Facebook, Inc.	No. 1:18-cv-06774-RJS	07/27/2018	Southern District of New York
3.	Kacouris v. Facebook, Inc.	No. 1:18-cv-06765-RJS	07/27/2018	Southern District of New York
4.	Casey v. Facebook Inc.	No. 5:18-cv-01780-EJD	03/22/2018	Northern District of California
5.	Ernestine v. Facebook, Inc.	No. 3:18-CV-01868-EJD	03/27/2018	Northern District of California
Derivative Litigation				
6.	Feuer v. Zuckerberg et al.	No. 2019-0324	05/01/2019	Delaware Chancery Court
7.	Hallisey v. Zuckerberg	No. 4:18-cv-01792-HSG	03/22/2018	Northern District of California
8.	Martin v. Zuckerberg	No. 4:18-cv-01834-HSG	03/23/2018	Northern District of California
9.	Ocegueda v. Zuckerberg	No. 4:18-cv-01893-HSG	03/27/2018	Northern District of California
10.	Karon v. Facebook, Inc.	No. 4:18-cv-01929-HSG	03/29/2018	Northern District of California
11.	Gloria Stricklin Trust v. Zuckerberg	No. 4:18-cv-02011-HSG	04/02/2018	Northern District of California
12.	Sbriglio v. Zuckerberg, et al.	No. 2018-0307-JRS	04/25/2018	Delaware Chancery Court
13.	In re Facebook, Inc. Shareholder Derivative Privacy Litigation	No. 4:18-cv-01792-HSG	03/22/2018	Northern District of California
14.	O'Connor v. Zuckerberg, et al.	No. 19-CIV-03759	06/28/2019	San Mateo Superior Court
15.	Chase v. Zuckerberg, et al.	No. 4:18-CV-03710-HSG	04/18/2018	Northern District of California
16.	Leagre v. Zuckerberg, et al.	No. 2018-0675-JRS	09/13/2018	Delaware Chancery Court

[1] This field represents the court of original filing or the court where the case has been consolidated and is now pending. For example, the consumer-based lawsuits were filed in courts across the country, and many have been consolidated in a multidistrict litigation pending in the U.S. District Court for the Northern District of California.

Representative Litigation Relating To Cambridge Analytica Events

Books-and-Records Litigation				
17.	In re Facebook Inc. Section 220 Litigation	C.A. No. 2018-0661	09/06/2018	Delaware Chancery Court
18.	Ocegueda v. Facebook, Inc.	No. 18-CIV-04936	09/14/2018	San Mateo Superior Court
19.	City of Birmingham Relief and Retirement System v. Facebook, Inc.	No. 2018-0532	07/23/2018	Delaware Chancery Court
20.	Levy v. Facebook, Inc.	No. 2018-0705	09/28/2018	Delaware Chancery Court
Consumer-Based Litigation				
21.	Price v. Facebook, Inc.	No. 3:18-cv-01732-VC	03/20/2018	Northern District of California
22.	Rubin v. Facebook, Inc.	No. 3:18-cv-01852-VC	03/26/2018	Northern District of California
23.	O'Kelly v. Facebook, Inc.	No. 3-18-cv-01915-VC	03/28/2018	Northern District of California
24.	Beiner et al. v. Facebook, Inc.	No. 3:18-cv-01953-VC	03/29/2018	Northern District of California
25.	Gennock et al. v. Facebook, Inc.	No. 3:18-cv-01891-VC	03/27/2017	Northern District of California
26.	Haslinger v. Facebook, Inc.	No. 3:18-cv-01984-VC	03/30/2018	Northern District of California
27.	Kooser et al. v. Facebook, Inc.	No. 3:18-cv-02009-VC	04/02/2018	Northern District of California
28.	Picha v. Facebook, Inc.	No: 3:18-cv-02090-VC	04/05/2018	Northern District of California
29.	Labajo v. Facebook, Inc.	No. 3:18-cv-02093-VC	04/05/2018	Northern District of California
30.	Iron Wing et al. v. Facebook, Inc.	No. 3:18-cv-02122-VC	04/06/2018	Northern District of California
31.	Johnson et al v. Facebook, Inc.	No. 3:18-cv-02127-VC	04/09/2018	Northern District of California
32.	Buckles v. Facebook, Inc.	No. 3:18-cv-02189-VC	04/12/2018	Northern District of California
33.	Gerena v. Facebook, Inc.	No. 3:18-cv-02201-VC	04/12/2018	Northern District of California
34.	King v. Facebook, Inc.	No. 3:18-cv-02276-VC	04/16/2018	Northern District of California

Representative Litigation Relating To Cambridge Analytica Events

35.	Diaz Sanchez v. Facebook, Inc.	No. 3:18-cv-02381-VC	04/20/2018	Northern District of California
36.	Schinder v. Facebook, Inc.	No. 3:18-cv-02571-VC	05/01/2018	Northern District of California
37.	Pelc v. Facebook, Inc.	No. 3:18-cv-02948-VC	05/18/2018	Northern District of California
38.	Malskoff et al. v. Facebook, Inc.	No. 3:18-cv-03393-VC	03/27/2018	Northern District of California
39.	Burk et al. v. Facebook, Inc.	No. 3:18-cv-02504-VC	04/26/2018	Northern District of California
40.	Comforte et al. v. Facebook, Inc.	No. 3:18-cv-03394-VC	03/22/2018	Northern District of California
41.	Hassan et al v. Facebook, Inc.	No. 3:19-cv-01003-VC	02/22/2019	Northern District of California
42.	Lodowski v. Facebook, Inc.	No. 3:18-cv-03484-VC	03/23/2018	Northern District of California
43.	Burton v. Facebook et al.	No. 3:18-cv-03643-VC	04/12/2018	Northern District of California
44.	Redmond et al. v. Facebook, Inc.	No. 3:18-cv-03642-VC	04/10/2018	Northern District of California
45.	Williams v. Facebook, Inc.	No. 3:18-cv-03676-VC	04/04/2018	Northern District of California
46.	O'Hara et al. v. Facebook, Inc.	No. 3:18-cv-03709-VC	04/04/2018	Northern District of California
47.	Vance-Guerbe v. Facebook, Inc.	No. 3:18-cv-02987-VC	05/21/2018	Northern District of California
48.	Bouillon v. Facebook, Inc.	No. 3:18-cv-02565-VC	05/01/2018	Northern District of California
49.	Skotnicki v. Facebook, Inc.	No. 3:18-cv-03790-VC	04/30/2018	Northern District of California
50.	Reninger v. Facebook, Inc.	No. 3:18-cv-04089-VC	06/21/2018	Northern District of California
51.	Kopecky v. Facebook, Inc.	No. 3:18-cv-04125-VC	06/19/2018	Northern District of California
52.	Akins et al. v. Facebook, Inc.	No. 3:18-cv-05714-VC	09/18/2018	Northern District of California
53.	Kmieciak et al. v. Facebook, Inc.	No. 3:18-cv-05752-VC	09/19/2018	Northern District of California
54.	Staggs et al. v. Facebook, Inc.	No. 3:18-cv-05754-VC	09/19/2018	Northern District of California

Representative Litigation Relating To Cambridge Analytica Events

55.	Miller et al. v. Facebook, Inc.	No. 3:18-cv-05770-VC	09/20/2018	Northern District of California
56.	McDonnell et al. v. Facebook, Inc.	No. 3:18-cv-05811-VC	09/21/2018	Northern District of California
57.	Rankins v. Facebook, Inc.	No. 3:18-cv-05380-VC	08/31/2018	Northern District of California
58.	Hwang v. Facebook, Inc.	No. 3:18-cv-05357-VC	08/30/2018	Northern District of California
59.	Ballejos et al. v. Facebook, Inc.	No. 18-CIV-03607	07/11/2018	San Mateo Superior Court
60.	Zimmerman et al. v. Facebook, Inc.	No. 19-04591	08/07/2019	Northern District of California
61.	People of the State of Illinois v. Facebook, Inc.	No. 18-CH-03868	03/23/2018	Cook County Circuit Court
Offensive Litigation Involving Developers				
62.	Facebook, Inc. v. Rankwave Co.	No. 4:19-cv-03738-JST	05/10/2019	Northern District of California
Defensive Litigation Involving Developers				
63.	Six4three, LLC v. Facebook, Inc.	No. 3:17-cv-00359-WHA	04/10/2015	Northern District of California
64.	Aleksandr Kogan v. Facebook, Inc.	No. 19-cv-2560 (PAE)	03/15/2019	Southern District of New York
Regulatory Litigation				
65.	District of Columbia v. Facebook, Inc.	2018 CA 008715 B	12/19/2018	Superior Court of the District of Columbia

Volume: 1
Pages: 1-127
Exhibits: See Index

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, SS. SUPERIOR COURT DEPARTMENT
OF THE TRIAL COURT

****
*
ATTORNEY GENERAL'S OFFICE, *
Plaintiff, *
*
vs. * Docket No. 1984CV02597
*
FACEBOOK, INC., *
Defendant. *
*
****

RE: MOTION HEARING
BEFORE THE HONORABLE BRIAN A. DAVIS

APPEARANCES:

For the Plaintiff:
Office of the Attorney General
By: Sara E. Cable, Assistant District Attorney
By: Jared Rinehimer, Assistant District Attorney
By: Peter Downing, Assistant District Attorney
One Ashburton Place
Boston, Massachusetts 02108
617.963.2827

Appearances Continued on page 2.

Boston, Massachusetts
Courtroom 1309
November 7, 2019

Court Transcriber: Lisa Marie Phipps, Certified Shorthand Reporter, Registered Professional Reporter, Certified Realtime Reporter

APPEARANCES (Continued):

For the Defendant:
Wilmer Cutler Pickering Hale and Dorr LLP
By: Felicia H. Ellsworth, Esquire
By: Rachel Lee Gargiulo, Esquire
By: Eric Lloyd Hawkins, Esquire
60 State Street
Boston, Massachusetts 02109
617.526.6687

For the Defendant:
Gibson Dunn
By: Alexander H. Southwell, Esquire
By: Amanda M. Aycock, Esquire
200 Park Avenue
New York, New York 10166
212.351.4000

I N D E X

WITNESS:

(None.)

EXHIBITS:

(None.)

FOR IDENTIFICATION:

(None.)

P R O C E E D I N G S

(Court called to order.)

(2:05 p.m.)

THE COURT OFFICER: Court's in session, please be seated.

THE COURT: Good afternoon, everyone. Welcome.

THE CLERK: Calling Civil Action No. 20192597, Attorney General versus Facebook.

Counsel, please identify yourselves for the record.

MS. CABLE: Good afternoon your Honor.

Sarah Cable for the Attorney General's Office.

THE COURT: Ms. Cable, welcome back.

MR. RINEHIMER: Jared Rinehimer for the Attorney General's Office.

THE COURT: Mr. Rinehimer, welcome, sir.

MR. DOWNING: Peter Downing for the Attorney General's Office.

THE COURT: Mr. Downing, welcome.

MS. ELLSWORTH: Good afternoon, your Honor, Felicia Ellsworth for Facebook.

THE COURT: Ms. Ellsworth, welcome back.

MS. ELLSWORTH: And I'm joined by Alex

Southwell from Gibbs and Dunn, also here for Facebook.

MR. SOUTHWELL: Good afternoon, your Honor.

THE COURT: Sir, welcome.

And, sir, do you have an appearance in?

MR. SOUTHWELL: Yes, your Honor, I've been admitted pro hac.

THE COURT: Last name again?

MR. SOUTHWELL: Southwell.

THE COURT: Mr. Southwell.

MR. SOUTHWELL: S-O-U-T-H-W-E-L-L.

THE COURT: Got it. And you're here -- are you here from California?

MR. SOUTHWELL: No, your Honor. I sit in New York.

THE COURT: In New York, close enough.

And who is in back?

MS. ELLSWORTH: In the back, your Honor, we have Mr. Hawkins, Ms. Gargiulo, and Ms. Aycock also representing Facebook.

THE COURT: Got it.

MS. ELLSWORTH: Ms. Aycock was recently pro haced in, and Mr. Hawkins and Ms. Gargiulo have appearances.

THE COURT: Yes. I've got it.

Welcome, everyone.

Folks, we are here, it took a little while, but we are here to talk about the petition and enforcement of the petition.

I've read the papers. So -- and I read the papers in part so that we can go directly to the issues that we need to discuss.

So I suspect that maybe people have presentations that they want to make to me, and I see some boards off to the side.

So -- but, as a general matter, what I like to do is jump into the issues as quickly as we can.

But let me -- before I do that, is there anything we need to address in advance of discussing the issues?

Ms. Cable, anything?

MS. CABLE: I think we're ready.

THE COURT: If you would just stand when you speak, if you don't mind.

MS. CABLE: Sorry, no. I think we are ready to jump into the issues, your Honor.

THE COURT: Okay.

And, Ms. Farnsworth, anything?

MS. ELLSWORTH: No, nothing further.

THE COURT: Ms. Ellsworth. Yes? No? Nothing?

All right. Then let me start with the Attorney General.

Ms. Cable, here's what I am trying to understand what it is that you are looking for. It's not entirely clear, I have to say, even from reading the papers, because you incorporate by reference some of the categories of the CID.

And we are only talking about the third CID; is that right?

MS. CABLE: That's correct.

THE COURT: So we're only talking about the third CID.

And when -- on my first pass at reviewing, again, your prayers for relief and the like, were like -- what you really need -- and I thought I had some recollection from our prior get-together on this, because we have been together on this when we were talking about impounding specific portions of the petition and the exhibits, that what you were really looking for, is you were looking for the app names and the app developers and that would be enough just

to get that information.

Am I wrong?

MS. CABLE: We -- you're right in part. So the issue before impoundment --

THE COURT: That's a nice way to put it. Go ahead. Yes.

MS. CABLE: The issues that -- the app names feature prominently in the impoundment motion because that was one of the aspects that was at issue.

In addition to the app names, we are also seeking information about the apps, their certain characteristics about them, including their activity on the platform.

I think the best place, what I might suggest, if the Court has the petition in front of it --

THE COURT: I do.

MS. CABLE: -- is to look at Exhibit A, which is CID.

And if you go to page 9 and 10, which are requests --

THE COURT: So Exhibit A. So we are looking at the actual binder.

So, yes, 9 and 10, yep.

MS. CABLE: Page 9 and 10. It's Request 1, 2, and 3; and then on page 11 is Request 6.

THE COURT: Yes.

MS. CABLE: Now, what these are -- what these requests are looking for are the identity by name of certain apps. That's Request 1.

THE COURT: That fall within these specific groups.

MS. CABLE: That fall within the perimeters of Request 1.

MS. CABLE: And then as to those apps, the information listed in 2A through 2H. So that's, you know, information about those apps.

THE COURT: Um-hum.

MS. CABLE: And then on Request 3, the identification of apps that fall within the perimeters of the categories of 3A, B and C.

THE COURT: Um-hum.

MS. CABLE: And on -- I'm sorry, also Request 4 then mirrors Request 2, so it requests that basic information about those apps, if I have that right.

Oh, no, sorry, counsel -- my co-counsel is telling me 4 is not an issue.

THE COURT: Four -- so you are not

looking what's -- and again, it's a -- part of, I guess, my confusion was, I looked at your prayer for relief --

MS. CABLE: Yep.

THE COURT: -- in your petition, which I think does make some effort to, I think, independently define what it is that you are looking for.

MS. CABLE: Yep.

THE COURT: And then I tried to match it up with what was contained in the CID, and it wasn't that -- and I couldn't make the direct correspondence.

MS. CABLE: Yep.

THE COURT: What I -- what I came away with is -- so, yes, you are looking for specific information about apps that fall within these particular categories.

And there's this -- for example, the 6,000; and then there are additional apps that are, again, based upon Facebook's past investigative experience, supposedly present this elevated risk.

And then we've got some others that there have been a detailed background check on or the

like; and so I am going -- I don't know exactly how I correlate those to the CID.

MS. CABLE: Let me -- let me try --

THE COURT: But I was working off -- primarily off of the prayer for relief.

MS. CABLE: Let me try to fit the prayer for relief into the CID.

At the time we issued the CID, which was November of 2018, we didn't know much about the ADI.

We were trying to -- and -- and to take a step back, we had asked for this information in a prior CID in the summer of 2018.

THE COURT: The same information that's in 3?

MS. CABLE: Similar information, but conceptualized differently.

Facebook refused to produce that information on the similar grounds that this was all collected or related to the ADI, unless there was a work product issue.

We then had a series of letters, and the Court has those, where we tried to -- we said, Let's learn a little more about the ADI so we can gauge whether or not this is a valid objection or

not.

Through those discussions, Facebook revealed that there were various phases of the ADI and various methods used to whittle down what we understood to be a huge number of apps into smaller categories.

Our effort in the CID that's before the Court that we are seeking to compel compliance with, was our attempt to fit our requests into the parlance that Facebook had been using so that they understood what we were looking for.

Between issuing this CID and, you know, the last few months, we learned a little more about the ADI.

And we obtained information from Facebook that told us there actually were even sub -- smaller categories of apps, because, again, you know, lists of millions of apps is not -- if that's what there is, great, but if we can get to a more narrow list that actually focuses on what we are concerned about, that's what we want.

So the prayer for relief is represent -- our attempt to ask for what Facebook told us existed.

We think that the petitions prayer for

relief is responsive to Requests 1, 2, 3, and 6 of our CID; but they are a subset of what we've requested.

So we are not seeking different information from our CID, we're seeking a different universe.

THE COURT: I guess that wasn't the focus of my discussion -- my questions.

I guess I'm less concerned, because having looked at the third CID, my quick take on it was what's requested in the prayer for relief is a subset --

MS. CABLE: Um-hum.

THE COURT: -- of what is requested in the third CID.

MS. CABLE: That's accurate.

THE COURT: What I was trying to determine is what has been peeled off, what you are not seeking anymore.

So, for example, there's a lot of discussions in the papers about communications which I think is really your -- it's the sixth category of your CID, which is referenced in the prayer for relief, all internal communications and internal correspondence concerning the apps

identified in response to Requests Nos. 1, 3, and 4.

You're still looking for that?

MS. CABLE: That's correct. And I'll note that those communications include those that predate the ADI.

THE COURT: Got it. So, for example, I am, you know, trying to understand the world here and what we are fighting about.

As I understand it, part of what you want is you want, again, the lists of apps that fall into these categories.

You want specific information about those apps as defined in the CID, the categories of the CID.

You want, for example, identification of the developers.

And I -- and what I take from your prayer for relief as well is you are looking for some description, and it may be -- you know, again, I am not exactly sure how it would be conveyed, but some description as to why it is that that app is of concern?

MS. CABLE: Yeah. And I think you are referring to Request 2E, the basis and initial

source?

THE COURT: Yeah. Or 4 -- for example, I look at 4B, which says that each app that was suspended and -- I'm sorry, I thought there was a reference to why they were suspended. So maybe it is 2B.

MS. CABLE: I think 2E is the basis and initial sorts of --

THE COURT: Yes. Okay.

MS. CABLE: Yeah. I mean, that is simply saying it -- you know, did you have reason before the ADI to suspect some data misuse here? What was the initial source of your concerns?

Was it through the ADI? In which case through the ADI is the answer. Or is it some reason prior to the ADI.

Were they on notice at some point before they initiated this investigation that there were particular apps that had engaged in misconduct and did they turn a blind eye to it. That's what that's going towards.

THE COURT: Got that. But, in addition, what you are also looking at is the apps themselves.

And what I came away with from our last

encounter was that what the AG has in mind is doing, perhaps, its own review of some of these apps --

MS. CABLE: Right.

THE COURT: -- to determine independently whether they present a problem.

MS. CABLE: Exactly.

THE COURT: And which -- and so are you looking for Facebook to provide you with some description as to why it is that Facebook has placed these particular apps in these particular categories?

MS. CABLE: I don't think that's exactly what we were looking for. I think we are looking for -- in our prayer for relief, there is some body of apps, at least 10,000 of which Facebook has some reason to suspect data misuse.

We are looking for identity of those apps, the developer, the basic information about whether it was released to the public and when; how much data it had; how many people were effected; and whether or not its concerns stem from the ADI or for some other reason.

THE COURT: All right.

MS. CABLE: And to the extent it's some

other reason, it -- that doesn't fall on the ADI, you know, I see -- we would want to know that reason.

I don't know that there would be objection under the work product doctrine to produce that information. So, yes, we would want that information.

I think I recognize if it's not identified until the ADI, there may be some work product elements to it.

I don't have a factual record to even be able gage that. I mean, this is speculating on my part, but yes.

THE COURT: Because you cast a very broad net in Category 6.

And, again, what I was also trying to understand is what is it that you are looking for in Category 6 that you don't think you pick up or that -- you know, what are you looking for in Category 6 --

MS. CABLE: I think the --

THE COURT: -- because your other categories it's sort of specific.

MS. CABLE: Uh-hum.

THE COURT: And then 6 casts this very

wide net that says we all want --

MS. CABLE: So --

THE COURT: -- all internal communication.

So I took from that is you want all the chatter within Facebook and within, for example, the ADI about what is it about this app that causes us to flag it?

MS. CABLE: And I think I could take a step back and look at this scenario that prompted our investigation in the first place.

This issue with the app selling data to Cambridge Analytica.

There's one app that sold data of 87 million users' information. One app.

THE COURT: I thought it was 88, but okay, we'll take 87.

MS. CABLE: I'll give you a million, yeah.

And there are 7 to 9 million apps on the platform at the same time who theoretically had access to the same amount of data.

With respect to Cambridge Analytica, Cambridge Analytica was kicked off the platform only after there was press attention around it.

There were media reports.

We've now learned, and it's in the petition --

THE COURT: Right. And I've read it. I've got it.

So you are going back to the prior occasion when they were asked to confirm, to certify, that they destroyed the data?

MS. CABLE: Yeah. Exactly.

THE COURT: Got it.

MS. CABLE: There's some indication that they actually were on notice well before 2015; that Cambridge Analytica was potentially engaged in some sort of wrongdoing. They didn't do anything about it.

And in the papers we suggest that maybe they were trying to keep Cambridge Analytica on board as an advertiser.

So I think the theory behind No. 6 is, if you have an app and the app is engaged in some conduct in 2013, 2014, where you were on notice that they were violating your Data Use Policies, that they were taking consumers data and selling it or using it in ways that the consumer didn't consent to, did you take action?

Because they had policies in place that purported that they would take action.

THE COURT: But 6 is a lot broader than that, isn't it? I mean, again, you are asking -- I understand 6.

It says, "all internal communications concerning the apps."

So what I read that to mean is, so there are certain apps that have been identified -- perhaps they were identified prior to the ADI -- but there are certain apps identified.

It's very clear your CID is also focusing on apps that have been identified in the ADI.

MS. CABLE: Um-hum.

THE COURT: And then you want all the internal communications about those apps, which I guess would mean everything that's gone back and forth within Facebook --

MS. CABLE: Yeah.

THE COURT: -- and it's part of the ADI concerning -- so what is it that, again, causes that app to the best of concern; what steps do we think we are going to take? You want all of that?

MS. CABLE: I think the practicalities of

responding to this are something we are happy to meet and confer with Facebook. And if we need to meet -- and we haven't yet.

THE COURT: Yes.

MS. CABLE: Because of this issue. This issue has prevented us from having discussions --

THE COURT: "This issue" being the assertion of the work product and attorney client privilege?

MS. CABLE: Right. Right. Because the body of apps that 6 would respond to turns in part to whether they can refuse to identify those apps to us.

So we are happy to have discussions about the practicalities of No. 6, including maybe some logical limits around it. We just haven't gotten there yet.

And it's -- frankly, there's no -- it's not before the Court today. It's not been briefed.

It's a fight for another day, perhaps, but...

THE COURT: All right. I am going to come at it from a different direction.

Are you looking for -- so it's Gibbs and

Dunn? Gibbs and Dunn is the firm that's doing -- working with Facebook on the ADI; is that right?

MS. ELLSWORTH: That's correct, your Honor.

MS. CABLE: Yes.

THE COURT: Okay. So are you looking for, as part of, as being responsive to your category No. 6, any memoranda that Gibbs and Dunn has prepared where Gibbs and Dunn assesses the litigation risk to Facebook on account of a particular app?

MS. CABLE: Our CID allows Facebook to withhold that as privilege provided they produce a privilege log, which they have not done here.

THE COURT: So you're not arguing that that information is not privileged?

MS. CABLE: No.

THE COURT: So there is a dividing line in there somewhere.

And you see, again -- since I am being asked to determine what falls on which side of the line, the dividing line is, again, anything that would be communications between Facebook and Gibbs and Dunn regarding litigation risks,

litigation exposure, litigation strategy, you are not looking for?

MS. CABLE: We've not sought that, your Honor.

THE COURT: Are you looking for any assessments by Gibbs and Dunn as to whether a particular app should be kicked off the platform?

MS. CABLE: Not the assessments themselves. Facebook has identified the apps that have been kicked off. So we have that information; but, no, we are not seeking an inner line assessment.

THE COURT: Are you looking for the assessments of any technical advisors?

So there is a reference in the materials -- Facebook says that they've been doing this for a while and they -- previously they had this work done by -- I think it was called the -- let me make sure I got it right here.

Is it the OpsDev team?

MS. CABLE: The DevOps.

THE COURT: DevOps, I got it. I got it backward.

MS. CABLE: DevOps. DevOps, I think is

the word. Yeah.

THE COURT: Sorry. So the DevOps team. So are you looking for assessments by the Dev -- by the DevOps team or the equivalent of the DevOps team as to why a particular app should be kicked off of the platform?

MS. CABLE: Not -- not in Requests 1, 2, 3 or 6. We are looking for facts. The identity of the apps and facts about those apps.

THE COURT: Got it. Okay.

Anything else, Ms. Cable, that you want to share with me right now, because I am going to turn to Ms. Ellsworth in a moment?

MS. CABLE: Not at this time.

THE COURT: All right.

Ms. Ellsworth, your arguing.

MS. ELLSWORTH: Yes, your Honor, although, with your permission, Mr. Southwell is here in case there are specific questions about details on the ADI that --

THE COURT: Good. Well, that's good. Thank you. Thank you for joining us.

MS. ELLSWORTH: -- he is better served. Yeah.

THE COURT: All right. Let me ask you

some questions about what's going on here.

MS. ELLSWORTH: Certainly.

THE COURT: So the ADI was instituted in March of 2018; is that right?

MS. ELLSWORTH: Correct. March and April, essentially.

THE COURT: If I read the papers correctly, Facebook doesn't dispute that it had its own enforcement program in place to police apps, an app compliant with Facebook policies prior to March of 2018; is that right?

MS. ELLSWORTH: That's correct. This is a different enterprise.

THE COURT: Well, but performing the same function?

MS. ELLSWORTH: I -- I would disagree with that, your Honor. I mean, and we put this forth in the declaration of Ms. Chen.

THE COURT: And I've read Ms. Chen's...

MS. ELLSWORTH: Understood, your Honor.

THE COURT: But it sounds like -- if I read her -- read her declaration correctly, she says, Listen, we used to do this, we used to have the DevOps team do this.

Beginning in March of 2018, we had Gibbs

and Dunn and the people that Gibbs and Dunn selected do this.

MS. ELLSWORTH: Not precisely, your Honor. So beginning in March --

THE COURT: Well, how am I wrong?

MS. ELLSWORTH: So beginning in March of 2018, when the investigation was commenced, Gibbs and Dunn, as well as the forensic investigators and others, began a backwards-looking analysis of legal risks that might entail from potential data misuse looking for --

THE COURT: But they are not looking for what has to do with legal risks.

So they -- you don't have to worry about -- Ms. Cable's already indicated she is not looking for -- the AG's not looking for communications where there is an assessment of legal risk.

MS. ELLSWORTH: But the --

THE COURT: The question is about compliance.

So OpsDev -- that question is whether apps comply, and perhaps some indication is why they may not comply.

MS. ELLSWORTH: But the entirety of ADI,

your Honor, is actually looking at legal risks that may come from whatever apps have been doing or not doing vis-à-vis Facebook's privacy policy.

THE COURT: Is the ADI performing any of the tasks that were previously performed by the DevOps team?

MS. ELLSWORTH: I think to answer that correctly, I would have to say, yes, in part, DevOps had tasks that were similar to what ADI did.

And some of what DevOps did in the past would also be privileged, your Honor.

I mean, certainly to the extent that they are making assessments and escalating those to legal for purposes of suspending or taking other enforcement action against apps, there would be a claimed privilege over some of those in the future.

THE COURT: Well, when you say when they send them to legal, so when they are requesting legal advice?

MS. ELLSWORTH: Or when at the request of Facebook's in-house legal, the DevOps team may have looked at a particular app or types of apps.

So I don't think we would say that

nothing that DevOps did in the past or is doing now, because it exists as a separate going concern, doesn't implicate the privilege issues.

But -- but quite purposely the ADI is a classic privileged internal investigation into whether there was any other instances of data misuse like the Cambridge Analytical instance, right?

That is what spurred this. There is no dispute about that.

And the reason for it was for Facebook to be able to assess and ascertain whether there were other legal risks, either for Facebook to take offensive action against some entity that had misused in violation of Facebook's policies and platform, or in order to be prepared for and to defend against litigation and regulatory enforcement and other inquiries that they anticipated would come to pass and, indeed, did come to pass.

THE COURT: That's the only reason they are doing this?

MS. ELLSWORTH: It's to assess the legal risk associated with the ADI. And I would --

THE COURT: So, for example, Facebook is

not conducting the ADI because it has an obligation to its users to protect their privacy and police its platform?

MS. ELLSWORTH: It's both, your Honor, but that doesn't divorce it -- or it doesn't divest of its privileged nature.

THE COURT: I'm not sure that's correct.

MS. ELLSWORTH: Well, I look at Comcast, your Honor --

THE COURT: Hmm.

MS. ELLSWORTH: -- which is quite clear, that so long as something was taken because of litigation and because of legal risk, the work product applies there.

THE COURT: No, well, let's -- actually, you are going exactly where I'm going.

So let's -- let's pause and talk about Facebook for the moment -- talk about Comcast for the moment, because Comcast says, absolutely, that if it's -- that's the because-of test.

MS. ELLSWORTH: Correct, your Honor.

THE COURT: But I -- maybe we are applying the because-of test differently here.

Comcast also says that if the work -- so I am on Page 318, and here it's quoting from

United States v. Textron.

And recall, Comcast, we talked about that Anderson -- Arthur Anderson memo.

MS. ELLSWORTH: Um-hum.

THE COURT: So it was in the context of accounting advice.

But the question was, it says, Stated differently, the Anderson memoranda or their substantial equivalent would not have been prepared irrespective of the prospect of litigation.

So what the -- flipping that around, looking at the -- that from the other side, what the SJC is saying is that if the information or the -- its substantial equivalent would have been generated irrespective of the litigation, it's not protected.

Do you agree with that proposition?

MS. ELLSWORTH: Well, I'm not sure I would phrase it exactly that way.

But I think irrespective of how we phrase it, what Facebook did here, and what Ms. Chen lays out in her declaration, was very different from what DevOps was doing.

Now, there's some overlap --

THE COURT: Pause for a moment. I'll give you the opportunity. And you should know I've read the papers.

MS. ELLSWORTH: Yeah, I understand.

THE COURT: And I understand your position, that it is different.

MS. ELLSWORTH: Right.

THE COURT: What I want to start with is, do you agree that if Facebook would have undertaken a review of these apps, irrespective of the ADI, then it's not protected by the work-product doctrine?

MS. ELLSWORTH: I don't agree with that, your Honor, because the anticipation of litigation is what spurred the ADI on. So I think there's a --

THE COURT: If -- again, again, you are not -- you're -- I'm sorry, but twisting the question a little bit.

My question is, we are talking here really about system maintenance, aren't we? So Facebook has to ecosystem; and one of the things on the ecosystem is the platform, and there are apps on the platform.

And as I understand the papers, what

Facebook has to do and has -- it claims, for example, in 2017, that you threw like 370 apps off the platform because they were policing the system.

So Facebook does routine -- as part of its routine maintenance of its ecosystem, it examines apps, it determines whether they are in compliance.

And if they are not in compliance, I'm not exactly sure they all get kicked off the system, but some number of them get kicked off the system.

Do I have that correct?

MS. ELLSWORTH: That is correct as a matter of maintenance.

What is different about what the ADI is, is that it is a comprehensive review of everything, as opposed to somebody flags an issue and then that is looked into, right.

THE COURT: Is it fair to characterize it as a better maintenance program?

MS. ELLSWORTH: I -- it is certainly more robust and far-reaching than what was in place at the time.

Whether it's --

THE COURT: Is it a maintenance program?

MS. ELLSWORTH: I wouldn't call it a maintenance program.

And, again, I don't mean to quibble on the words; but I do think it matters that Facebook took a step back and said, Unlike what we normally do, which is to just let things bubble up and take action it arises --

THE COURT: Well, is that true? I don't take that from your papers.

It doesn't sound like -- again, Facebook is making representations that they are affirmatively out there prior to March of 2018 looking at apps, and confirming that they are in compliance.

Are you saying that it's only things that bubbled up that Facebook took any action on prior to March of 2018.

MS. ELLSWORTH: Well, I think it is not -- it was not the case that prior to March 2018 every app on the platform would be reviewed by the DevOps team on some sort of regular basis.

They were reviewed as they come in.

THE COURT: But was Facebook taking

affirmative steps prior to March of 2018 to police apps?

MS. ELLSWORTH: It was taking affirmative steps to police apps, yes.

THE COURT: Okay.

MS. ELLSWORTH: It certainly was.

THE COURT: And, again, and I'm looking at the papers that you've given me.

So, for example, and I want to make sure I've got this right, Exhibit I to the petition, all right, is part of --

MS. ELLSWORTH: That's the August 2018 letter, your Honor?

THE COURT: Yes. Appendix A says, Facebook takes the protection of its users -- private -- information very seriously from Platform's inception.

So Platform Version 1 went into effect in roughly 2012.

Do I have that right?

MS. ELLSWORTH: Yep.

THE COURT: Although there's a reference in the papers to early apps, 2007, do I -- do I have that right?

MS. ELLSWORTH: I don't think that was

Platform, per se. It may have been some other --

THE COURT: There's definitely a reference to an app.

MS. CABLE: That's when Facebook might have been online versus an app on a Mobil device, perhaps.

THE COURT: I'm not sure. I thought it was maybe in Ms. Chen's declaration.

Well, I've got the dates right. So Version 1 --

MS. ELLSWORTH: Version 1, right.

THE COURT: -- of the Platform -- and we all know what we are talking about -- the Platform came online 2012.

MS. ELLSWORTH: That's correct.

THE COURT: All right. So it says, again, in this Exhibit A that Facebook takes the protection of users' information very seriously from Platform's inception, meaning 2012.

Facebook has had policies such as its terms of service; formally, the statement of rights and responsibilities, SRR, and Platform policy that govern the use of user data by third-party apps and developers.

It says, In parallel, Facebook has

implemented a wide rage of measures to monitor third-party apps and take action against apps and developers that do not comply with Facebook's policies. Let me stop there.

"In parallel," does that mean that in conjunction with the implementation of Version 1 of the Platform that Facebook implemented a wide range of measures to monitor third-party apps and take actions against apps and developers that do not comply with Facebook's policies?

Do I have that right?

MS. ELLSWORTH: That's correct, your Honor.

THE COURT: So prior to March of 2018, Facebook's on this. They are looking at apps; and they're trying to confirm that the apps comply with Facebook policies and that they don't compromise user privacy.

MS. ELLSWORTH: What is different about --

THE COURT: Wait. Wait. Before we move on --

MS. ELLSWORTH: I'm sorry. Go ahead. Yep.

THE COURT: -- do I have that right?

MS. ELLSWORTH: That's correct, your Honor. Yeah.

THE COURT: So -- and then it says -- then it goes on in the next paragraph, it says, In particular, Facebook has put in place an enforcement program to prevent and respond to potential developer misuse of user information.

Facebook has dedicated significant internal and external resources to this program, including for detecting, escalating, investigating, and combating violations of Facebook policies.

Is that something, that program, that enforcement program, did that exist prior to March of 2018?

MS. ELLSWORTH: It did. And, as I said, your Honor, some of the work that was done prior to March of 2018, likely is subject to claims of privilege and work product because it is attorney directed or provided legal advice.

THE COURT: Yeah. We'll get there.

MS. ELLSWORTH: Okay.

THE COURT: Because, again, there is a line here somewhere.

MS. ELLSWORTH: Um-hum.

THE COURT: And that's part of the reason why for my reason -- my questions to Ms. Cable.

It seems to me that there is some information here that may be protected. What I am trying to do is -- we are starting with work product.

I'm trying to understand what it is that we have in the ADI, because I read -- and I think we are governed here by Comcast, okay.

You are in a Massachusetts Superior Court, Massachusetts AG, CID, so I am going to say that I am governed by Commissioner of Revenue versus Comcast.

And I -- I interpret it somewhat differently than you do.

Comcast seemed to say quite explicitly that if the information, materials, would have been generated irrespective of the prospect of litigation, they don't fall within the work-product protection.

And what I'm trying to understand here is Facebook's efforts prior to March of 2018 to enforce, to police, to protect user privacy.

What I am hearing is, yes, it did have. It sounds like it had a rather elaborate

enforcement program in place for that purpose.

Do I have that right?

MS. ELLSWORTH: You do have that right. And it still does, and that exists separately from the ADI.

THE COURT: I see. It exists completely separately from the ADI?

MS. ELLSWORTH: Yes. There is a -- there's a separate ongoing enforcement of what we are talking -- today's Platform, enforcement work for the Platform today, which is not the Platform that ADI is focused on.

ADI is focused on the pre-2014 Platform, Version 1 (inaudible).

THE COURT: So is ADI -- is it fair to say that ADI is redoing some of the work that was done or perhaps should have been done the first time around?

MS. ELLSWORTH: I think without putting any sort of spin on that --

THE COURT: And I'm not -- I'm not trying to cast any accusations. I'm simply trying to understand what the ADI is about.

MS. ELLSWORTH: Yeah. And I understand that, your Honor.

Yes. I think it's fair to say that what the ADI is doing, it's a backwards looking at the V1 Platform, the pre-2014 version, to assess whether there is any incidents of data misuse, violations of Facebook's privacy policy; and to take action as a result, in conjunction with a consideration of legal risks.

The actions that have been taken have been shared with the Attorney General, suspension of 69,000 apps; request for information; litigation that we filed; all stemming from the work of the ADI.

THE COURT: Right.

MS. ELLSWORTH: Go ahead.

THE COURT: Here is what I'm going to do now.

MS. ELLSWORTH: Um-hum.

THE COURT: I'm going to be quiet. And I'm going to listen to you give me your best pitch as to why it is I should regard the ADI as a different animal, okay, as something different than the maintenance program that Facebook undertook, or should have undertaken, prior to March of 2018.

MS. ELLSWORTH: So I'll give you a few

reasons why I think you should view it as something different.

The first is the -- ADI was put into place by legal counsel; and it is attorney lead, attorney driven. That is different from the prior DevOps.

And that is not done to cloak it in privilege in order to avoid having to turn information over.

That was done --

THE COURT: Does it -- that's -- that has no -- that's not one of the reasons why it was done that way?

MS. ELLSWORTH: Well, it's a classic internal investigation.

THE COURT: I understand, but --

MS. ELLSWORTH: It's to look --

THE COURT: -- the question's different.

You are saying -- you just represented that that's not why they did it.

MS. ELLSWORTH: They didn't do it in order to avoid a CID from the Massachusetts Attorney General.

They did it in order to have the full and frank airing of potential legal risks that --

THE COURT: Okay.

MS. ELLSWORTH: -- Upjohn and all those cases --

THE COURT: People do that.

MS. ELLSWORTH: Yes.

THE COURT: Got it.

MS. ELLSWORTH: So, understood, your Honor's very familiar with those.

THE COURT: Yeah. You know, been there, done that. So I do understand why these investigations are undertaken sometimes by counsel.

MS. ELLSWORTH: Okay. The second point I would make is that the ADI is -- it's a closed-ended enterprise.

It is an -- it is an investigation that has a beginning, and it will have an end. It is ongoing as we stand here today. It has not yet ended.

But it is an ongoing investigation that will not sort of carry on to be the new enforcement rubric.

It will be ended as a legal investigation and the enforcement rubric, which has been going on in parallel by DevOps and then other teams

that are sort of its progeny is still ongoing.

And then I would point out that in Comcast, your Honor, what we were looking at there was a very different type of claim of work product, right.

That -- I know your Honor's familiar with the case. It is an accountant's memo.

The SJC expressly said had Comcast wanted to get a privileged assessment of its Massachusetts tax liability, it could have had a Massachusetts law firm provide that advice.

That is what Facebook did here. It had a law firm, Gibbs and Dunn, it engaged it in March of 2018 in order to design this investigation and to have this assessment of legal risk.

When there have been facts that have arisen from the investigation, those have been communicated publicly, including suspending apps, initiating litigation, other of the information that has been turned over without objection to the Attorney General's Office.

That is very different than the memo from Ernst & Young that's at issue in Comcast, right, it's an attorney-lead investigation.

And it was done so purposefully in order

to the type of full and frank disclosure that privilege and work product allows, which is recognized by all the courts, and which I won't reiterate for your Honor.

THE COURT: Um-hum.

MS. ELLSWORTH: So those are the primary differences, I would say, of the ADI and the prior and ongoing enforcement work.

It's similar to if there were an ongoing -- if there were an investigation of employee wrongdoing and legal counsel and HR come together to try and identify employees who may have engaged in some wrongdoing in a privileged investigation.

That doesn't mean that the human resources functions of the firm don't continue and continue to address other employee issues, right, it is a separate -- as I said, sort of closed-ended investigation that is doing some of the work that HR may have done in the past, but is doing some in a privileged manner to provide legal advice to the client.

THE COURT: I guess I would use a different analogy.

You bring your car in every 10,000 miles

for maintenance, inspection and maintenance, that's done by mechanics.

You hire an attorney to come in and inspect your car at 80,000 miles to do a thorough inspection and maintenance.

Does that make the maintenance work suddenly protected by the work-product doctrine?

MS. ELLSWORTH: No. But if you are a car manufacturer and you normally look at your cars as a matter of understanding improvements to them; and then you have your Ford Pinto explode, and then you have lawyers come in and conduct an investigation -- have the car manufacturer conduct an investigation into problems that Pinto may have had in the past, that would be a privileged exercise.

That's the type of legal risk and legal assessment that -- that internal investigations every day attempt to discern.

And you don't know what you are going to find when you start that investigation.

THE COURT: Okay. Anything else that you think I should know in order to distinguish the ADI from the enforcement programs that the -- the enforcement program that Facebook had in place

before?

MS. ELLSWORTH: Can I just confer for one moment, your Honor?

THE COURT: Yes, you may.

(Pause.)

MS. ELLSWORTH: I'll have Mr. Southwell add one thing, if you don't mind, your Honor.

THE COURT: Okay. Mr. Southwell.

MR. SOUTHWELL: Thank you, your Honor.

We would point your Honor to the Chen declaration, which I know you've reviewed in detail.

THE COURT: Yes, I've read it.

MR. SOUTHWELL: And I think that embodies the idea that there are substantial amounts of materials that were created for purpose of ADI.

And those are exactly the materials that are being sought by CID; and they are described in the Chen declaration clearly in an uncontested, factual way as something different than the materials that would have been created during a quote, unquote, maintenance-type approach.

THE COURT: See. But I read Ms. Chen's declaration and, for example, look at

paragraph 5, it says, For context, a legal-lead investigation is not Facebook's typical response when the company determines that violations of its Platform policies may have occurred, rather the developer operations, DevOps team, along with the policy team managing Facebook Platform policy have historically been the front lines to address potential violations of Platform policies in subsequent enforcement efforts.

So what I understand to be saying here, is that what the ADI is doing, is so they are replacing DevOps.

They're replacing DevOps in part because Cambridge Analytica blew up.

Do I have that right?

MR. SOUTHWELL: Respectfully, your Honor, you know, it's a slight tweak on that.

THE COURT: Yeah.

MR. SOUTHWELL: It's not a replacement of DevOps. I think as the Chen declaration, I think, attempts to layout, it is a new historical look back of the pre-2014 Platform done in a way that involves sophisticated outside forensic firms that do extensive -- and the Chen declaration details sort of the length of these

investigative reports that are being done as respect to the app activity, technical background.

That, I think, is detailed in the Chen declaration. And that is completely different and is not a replacement of DevOps and the way.

The DevOps work continues in the work that they do. And that is the material that the CID is seeking.

THE COURT: Uh-hum. Let me ask one quick question.

Maybe, Mr. Southwell, you may want to answer this or Ms. Ellsworth may, I'll leave it to the two of you to decide who handles this hot potato.

Is it Facebook's position that -- well, let me pause for a moment.

Cambridge Analytica, I think everybody agrees was an unhappy event. Okay.

Even Facebook, I think their papers would acknowledge an unhappy event.

MR. SOUTHWELL: Yes.

THE COURT: Is it Facebook's position, that but for, okay, the threat of litigation, Facebook would not have undertaken any enhanced

enforcement program in the aftermath of the Cambridge Analytica scandal? My word, not yours.

MS. ELLSWORTH: We'd certainly agree with your characterization of the unhappy event, your Honor.

THE COURT: Yes. Yeah, again, I don't think that anybody disputes that that was an unhappy event.

MS. ELLSWORTH: But -- but for the Cambridge Analytica events, Facebook would not have undertaken an investigation in this form, right?

THE COURT: But my question -- my question is different.

My question is, are you saying that Facebook would not have undertaken an enhanced enforcement program in the aftermath of Cambridge Analytica?

Are you saying wouldn't have done it? They would have just stayed the course, let DevOps figure it out? That's what they would have done?

MS. ELLSWORTH: But for the threat of litigation --

THE COURT: Correct.

MS. ELLSWORTH: -- that came from Cambridge Analytica, do you mean?

THE COURT: Yeah.

MS. ELLSWORTH: They would -- it would not have taken the form that it's taking, right?

It would not have involved these outside forensic consultants, which is not the normal force and not what -- -- not the normal course, excuse me, and not what is done in the daily --

THE COURT: So -- so, again, you are telling me, Facebook they wouldn't have brought in any additional resources; wouldn't have done much of anything different in the aftermath of Cambridge Analytica but for the threat of litigation?

MS. ELLSWORTH: I'm not necessarily saying that, your Honor, but I also don't know that one can sort of speculate about what we would have done but for the legal risks that were attendant.

THE COURT: But, see, I have to understand what Facebook may have done in circumstances.

And I have to say, I find it very difficult to believe that in the aftermath of

Cambridge Analytica -- where we can quibble about it, 87 or 88 million users information was disclosed -- that Facebook would not have taken -- undertaken some enhanced enforcement program but for the threat of litigation.

MS. ELLSWORTH: And I don't think, again, we both have read Comcast. But I don't think Comcast requires that, right?

Comcast makes clear that it need not be the primary purpose. It rejects that test.

THE COURT: Well, but it's because of, again, because of. So when -- this is the because-of test --

MS. ELLSWORTH: Um-hum.

THE COURT: -- which is, you are telling me that if they hadn't had the threat of litigation, the prospect of litigation, I think is the way it's phrased --

MS. CABLE: Um-hum.

THE COURT: -- in Comcast, wouldn't have taken -- wouldn't have undertaken any sort of enhanced enforcement program?

MS. ELLSWORTH: Well, enhanced enforcement program, I can't necessarily disagree with; but it wouldn't have undertaken the

enforcement program that it did, and it wouldn't have structured it the way it did.

THE COURT: All right.

MS. ELLSWORTH: I would point your Honor, and I know you are familiar with all the cases, but Judge Salinger's decision in the *America's Test Kitchen* case is a more recent sort of interpretation of Comcast.

We think that that also both guides what Facebook has done and shows why it's protected and also should guide your Honor's decision.

THE COURT: Shift gears.

You're claiming attorney client privilege --

MS. ELLSWORTH: Correct.

THE COURT: -- with respect to some of the materials.

It looks like the AG is conceding attorney-client privilege with respect to some materials.

So, for example, at least for current purposes, the AG is not looking for Gibbs and Dunn memos to Facebook regarding litigation risks associated with particular apps or groups of apps or the like.

So there doesn't seem to be any dispute. But that's some of what is happening as a result of the ADI would be protected.

But we are going back to the work that's generated on the enforcement -- investigation and enforcement side.

It appears as though Facebook is casting a sort of broad attorney-client privilege claim with respect to everything having to do with the investigation and enforcement.

Do I have that right?

MS. ELLSWORTH: That's right, your Honor.

THE COURT: Everything?

MS. ELLSWORTH: The investigation, yes.

THE COURT: Don't we face the same issue with respect to the attorney-client privilege claims?

Because if you look at *Chambers versus Gold Medal Bakery*, which is another SJC decision. This is a pretty recent decision -- I think it's 2013 -- *Chambers* says that the attorney-client privilege does not apply to information that would have been generated irrespective of litigation.

So it's really -- it comes down to the

same question, which is, if this work would have been done, irrespective of a threat or the prospect of litigation, you also can't cloak it in the attorney-client privilege.

Well, let me pause for a moment. I asked you before whether you would agree with me formulation on the work product side.

MS. ELLSWORTH: Yes.

THE COURT: Do you agree that that's what *Chambers* holds?

MS. ELLSWORTH: I'm not -- to be honest, your Honor, I'm not familiar with *Chambers*.

THE COURT: Yes.

MS. ELLSWORTH: But I certainly don't have a basis to disagree with the general principal, which seems accurate to me.

THE COURT: And I want to make sure. I want to be fair. So here's what -- in *Chambers* there was a question about this -- these were some directors trying to get access to information about the company when the directors were adverse to the company.

And on page 392 it's -- the SJC was sending the case back, I think they reversed and remanded.

They vacated and remanded, to the extent that's a difference, that makes a difference.

And they held that the judge or discovery master on remand should take particular care to distinguish Gold Medal's privilege communications with the law firm regarding the 2007 and present litigations from the underlying facts of Gold Medal's financial health and status, information that would have been generated irrespective of litigation.

This distinction a crucial because attorney-client privilege only protects against disclosure of confidential communications made to render legal services.

So it seems to me that what the SJC is saying there is if it's -- if you would have generated it, again, irrespective of litigation, or the prospect of litigation, it also doesn't fall within the scope of the attorney-client privilege.

Do you think otherwise?

MS. ELLSWORTH: I -- I think that that's different than what we are dealing with here with the lists that we are talking about and the information that's been compiled.

THE COURT: Yes. How?

MS. ELLSWORTH: Because the information -- these various different iterations of groupings of apps that Ms. Cable was talking about, those are the product of attorney decisionmaking, about whether --

THE COURT: Is that true at each level? So there are three levels, right, in the investigation process.

We've got like -- I think it's initial -- I know I've got them here somewhere --

MS. ELLSWORTH: Your Honor, I actually have -- if you don't.

THE COURT: -- it's detection and ID -- oh, we have a chart?

MS. ELLSWORTH: I have a chart. I've given it to Ms. Cable already.

THE COURT: I'm happy to have a chart.

MS. ELLSWORTH: I can hand it up. And there is a blowup of the same thing as well, in case --

THE COURT: Ms. Cable, counsel, you've seen this? Seen the chart?

MS. CABLE: Just before the hearing, yes.

THE COURT: Got it. Okay.

So let me see, we've got -- maybe -- and this may address. And we've got the big blowup version?

MR. SOUTHWELL: I'm not sure if your Honor can see that back there.

THE COURT: That's okay. I've got it in the chart form.

MS. ELLSWORTH: It's an attempt to catalog the CID requests on --

THE COURT: Yes.

MS. ELLSWORTH: -- 1, 2, 3, and 6 and into what -- the material that would actually be sought.

And so you were just talking about the different phases, the user impact and the categorical and the escalation method.

THE COURT: Well, actually, I am focusing on different phases.

MS. ELLSWORTH: Okay.

THE COURT: I understand that there are different tests that they use.

MS. ELLSWORTH: Um-hum.

THE COURT: Different means that they use to try to flag.

MS. ELLSWORTH: Correct.

THE COURT: And I think that's what you were referring to, like user impact and the like.

But as I understand it, ADI, first phase is detection and identification; then it's enhanced examination --

MS. ELLSWORTH: Correct.

THE COURT: -- and then it's enforcement.

MS. ELLSWORTH: Correct.

THE COURT: And I guess one of the questions I had, and then I'll be quiet again for a moment while you explain, is it wasn't clear to me that the attorneys had significant roles, at least in 1 and 2, other than perhaps sort of identifying, selecting people to work on 1 and 2 and helping to establish some of the policies and procedures to be followed in 1 and 2.

It appeared to me, based on the materials that I had, that the attorneys really become involved at the third phase.

Do I have that right?

MS. ELLSWORTH: That's not -- that's not accurate at all.

THE COURT: All right. Then explain -- how -- how do I have it wrong?

MS. ELLSWORTH: I'll endeavor to make it

clearer.

So the attorneys are involved -- certainly they were involved in the retention of the outside consultants and the directing of the work.

They are also involved at both Phases 1 and 2, right, detention and the escalation.

THE COURT: Doing what? What are the attorneys doing?

MS. ELLSWORTH: They are setting the perimeters. They are making -- as to the user impact method, which is one of the detection methods, they are deciding what the perimeters of number of users might be that would have an impact; and changing that as they make judgments about the legal risk that may entail from apps that they identify.

THE COURT: So they are establishing the protocols?

MS. ELLSWORTH: I would call them more than protocols. I would call them sort of perimeters that are potential risk sensitivities.

And those change and develop over time as the attorneys learn through the process of the investigation what, in fact, you know, the legal

risk that might be attendant. So they don't --

THE COURT: All right. And I don't want to put down Gibbs and Dunn attorneys, but I assume that most of the Gibbs and Dunn attorneys aren't the ones that are reviewing the source code and things of that nature to determine whether a particular app, for example, is tapping into -- improperly tapping into user data.

MS. ELLSWORTH: That's --

THE COURT: Again, maybe I'm wrong, but...

MS. ELLSWORTH: No, you are certainly right about that, although Mr. Southwell has many gifts.

They are looking -- they are telling -- that's why they engage the outside consultants --

THE COURT: Yes.

MS. ELLSWORTH: -- because they couldn't do that work, right, which is sort of like the classic example of that.

But they are working it iteratively and sort of all are part of the team. It's not just, okay, go do this and report it back.

It's do this, give me that information, okay, now do these five other things, and we may

have apps that fall off the list or come on to the list based on this changing of the risk assessments.

And it's going to be different for different apps.

And some of what we attempted to lay out in the papers and in the declaration is how that has evolved over time as the attorneys have understood the different risk perimeters to the company, both for data misuse and also for the legal risks that may attend.

THE COURT: Well, how is that different from, for example, attorneys all the time set guidelines -- they help draft guidelines for a corporation.

They don't question whether somebody is meeting the guidelines; whether someone has complied with the guidelines.

Is that protected as well simply because the attorneys establish the guidelines?

MS. ELLSWORTH: No. But the question -- in this circumstance, the question of whether somebody has complied with the guidelines, that output is on the end of the scale on this sort of suspension list.

It is when an app is suspended or has a sufficient level of suspicion based on the -- this iterative process with the attorneys where they're sent something like a request for information, right, in which the names of those apps have been provided to the Attorney General.

Anything that's an output of that process, as your Honor says, that's not going to be privileged or work product and we are not claiming that.

THE COURT: An "output" meaning that it is shared with a third-party --

MS. ELLSWORTH: It's shared with a --

THE COURT: -- right? Anything that's going, for example, to the developers --

MS. ELLSWORTH: Correct.

THE COURT: -- you are not claiming privilege?

MS. ELLSWORTH: No, and that's why we are --

THE COURT: And you are not claiming work product?

MS. ELLSWORTH: We are not claiming either. And that's why Request 4, I believe it is, or maybe request five, is not at issue

because those are external baseline communications.

THE COURT: So every -- every developer that has been notified already that it may have a problem -- again, no claim of privilege or work product with respect to those communications?

MS. ELLSWORTH: And the developers that have been notified have been notified in a variety of different ways, and they are at different stages of suspension or not depending on what they were trying --

THE COURT: So what we are really talking about are folks whose apps or names are being kicked around internally?

MS. ELLSWORTH: Or who -- an attorney thought might have something suspicious; and then maybe turned out to be wrong or maybe turned out to be right, and the app would go in a different direction depending on what the attorney's judgment was on that.

THE COURT: All right. So you said -- maybe I cut you off; maybe I didn't. I was trying to understand attorney involvement in the three phases.

So 1 and 2 -- again, if I understand it

correctly, you say they are setting perimeters, I use the term "protocols," but it's not the attorneys doing the busy work?

It's not the attorneys that are reviewing each of the apps and determining whether they meet the perimeters or the protocol?

That's all being done by either the technical experts, maybe it's being done by Facebook employees, don't know, it's not entirely clear; but, again, it's not the attorneys who are doing the technical review.

Do I have that right?

MS. ELLSWORTH: If the attorney says, I want to see all apps with 50 users or more, the attorneys are not looking to make sure that the name of an app provided actually has 50 users, that's correct.

THE COURT: Yeah. And I assume there is a lot of work associated with the ADI is somebody rolling up their sleeves and examining the apps and trying to understand how they operate and whether, again, they violate any of the protocols.

MS. ELLSWORTH: Well, it's -- I wouldn't go as far as the end of your sentence did, right?

It's the pulling information to report back to the attorneys, so the attorneys can then say, okay, This is cause for further suspicion.

THE COURT: Got it.

MS. ELLSWORTH: Let's continue to ask these five additional questions.

THE COURT: And it's only the attorneys making the call on whether these are suspicions?

MS. ELLSWORTH: Yes. That's correct, yes.

THE COURT: All right. Then I take it the attorneys have a much more prominent role in the enforcement phase?

MS. ELLSWORTH: The attorneys have a pretty in-the-weeds role throughout.

But when it comes to the actual enforcement phase, there are letters from Gibbs and Dunn that are sent out to the developers asking for information.

After an app has made it through this process such as there is sufficient need to find out how they are dealing with user data and complying with policies.

And, ultimately, it's Gibbs and Dunn, Facebook attorneys, that would make the

determination that either a failure to respond to that RFI or some other interaction with that developer is cause to put that app on the suspicion list and potentially to bring litigation against them.

THE COURT: Who made those calls prior to March of 2018?

MS. ELLSWORTH: The -- prior to March 2018, by the time you got to the enforcement phase, as we are calling it, it would have been attorneys as well.

It would be Facebook in-house legal at that point.

THE COURT: I see. All right.

MS. ELLSWORTH: As I said, the enforcement aspect of the Platform has always had some attorney involvement.

This is different and broader and deeper for all the reasons I've already articulated.

THE COURT: And have there -- let me clarify -- are the requests for this CID looking for information with respect to calls made by Facebook counsel prior to March of 2018?

So, for example, are we -- do we have at issue here what Ms. Ellsworth says are privileged

or work-product communications predating March of 2018 where an attorney, either Facebook in-house attorney or someone outside, made a determination on whether a particular app required some sort of enforcement action?

MS. CABLE: I don't know if we do. We don't have a privilege log. It hasn't come up.

We do have documents -- I don't know what level of completeness the production is -- but that do relate to enforcement steps or investigation taken by the DevOp team prior to the ADI.

So we do have, as a matter of fact, your Honor, we do have that information.

Whether they've withheld information, I don't know, because there's no privilege log.

THE COURT: I see.

MS. ELLSWORTH: The requests speak only to apps that have gone through one of these phases as a part of the ADI.

THE COURT: Hmm.

MS. ELLSWORTH: So it is not -- the way we've been interpreting the --

THE COURT: So your take on it is there's nothing in the CID that requests information

concerning pre-March of 2018 an -- investigation analysis enforcement; is that right?

MS. CABLE: According -- as to Requests 1 through 3, it all relates to the apps in the ADI.

The prior CIDs requested different activity, but we are focusing on the third CID.

As to Request 6, which is the all internal communications --

THE COURT: Yes.

MS. CABLE: -- it relates to apps that are in the ADI.

So it's the internal communications about apps that have been identified as a part of this investigation.

THE COURT: Um-hum.

MS. CABLE: But the time period spans back earlier than March of 2018.

THE COURT: All right. Again, we haven't seen it, and Ms. Cable is right, we don't have a privilege log here, which is something we'll turn to in a little bit.

But are all of the communications that are undertaken by members -- let's pause for a moment.

The ADI team consist of attorneys. As I

read Ms. Chen's declaration correctly, it consists of Gibbs and Dunn attorneys, it consists of some internal Facebook attorneys, including Ms. Chen, if I understand it correctly --

MS. ELLSWORTH: Correct.

THE COURT: And nonattorneys.

Do I have that right?

MS. ELLSWORTH: Certain nonattorney Facebook employees, correct. Yes.

THE COURT: Yes. And it looks like some outside consultants as well.

MS. ELLSWORTH: And the outside consultants from the two --

THE COURT: It looks like some outside help --

MS. ELLSWORTH: The two forensic firms, yes.

THE COURT: Then are all those communications -- there are attorneys on all of those communications.

So is -- is the protocol that somebody from Gibbs and Dunn, for example, is at least cc'd on every communication?

MS. ELLSWORTH: There probably are communications that attorneys are not on. That

doesn't divest them of privilege if they are taken to assist legal advice, as you know, nor would ccing them on every communication cloak them in privilege if they weren't --

THE COURT: I agree. I am just wondering what the protocol is.

MS. ELLSWORTH: -- in furtherance of legal advice.

THE COURT: So, and are you claiming attorney client communications with respect to all internal communications in the ADI?

MS. ELLSWORTH: In the ADI, yes.

THE COURT: Irrespective of whether attorneys are on those communications?

MS. ELLSWORTH: That's correct, your Honor.

THE COURT: You think each one would disclose legal advice or a request for legal advice?

MS. ELLSWORTH: Because the entirety of the ADI is to render legal advice and to provide assessment of legal risks, so, yes. That's what the ADI is doing.

And, you know, I understand that's what we are here to talk about, but that's -- that's

certainly our position.

THE COURT: Okay. So I'm looking at your chart.

Is there anything else that you want to bring to my attention?

MS. ELLSWORTH: Yeah, your Honor. I mean, the point of this chart was -- and I don't -- we don't have the prayers on there, although we did in a prior iteration, and maybe we should have kept them on, was simply denote what the breadth of what is actually sought by these aspects of the CID.

I would note, again, as to CID Request 3, we noted what we had actually produced, which is these categories about we're facing information.

But the rest of it is -- you know, these are lists that would not exist but for the involvement of attorneys.

This is not like a full document production, right?

So we do these as the equivalent of the binders of materials or of documents that have been selected by an attorney for further review as opposed to the entirety of the document production.

THE COURT: Got it.

Anything else?

MS. ELLSWORTH: I think that's all, your Honor.

THE COURT: Anything else you want to share with me, Ms. Ellsworth, on any --

MS. ELLSWORTH: No.

THE COURT: -- on any of the topics that we are discussing here today?

MS. ELLSWORTH: I'm happy to talk about the privilege log, if your Honor would like to speak about that now. You mentioned it.

THE COURT: Well, I just want to be clear. There is no privilege log. Nothing's been produced.

MS. ELLSWORTH: Nothing has been produced in response to the third CID over which -- well, we have produced in response to the third CID, but we informed the Attorney General's Office back in August of 2018 and, again, in December of 2018 -- that's exhibit OO and RR to the petition -- about the entirely privileged nature of this enterprise.

So it's -- you know, I can do a categorical privilege log --

THE COURT: So is it your position that a privilege log would itself be just an impossible undertaking?

MS. ELLSWORTH: It would be because it would be -- it would be everything that we're talking about today and we have provided -- in an effort to explain to the Attorney General why we take the position we do.

We have provided a lot of detailed information about why the ADI is privileged and why it is attorney work product in all those letters and in the oral briefings and telephone called and all that.

THE COURT: One further quick question for you.

I take it the -- if I'm correct, the Massachusetts Attorney General is not the only Attorney General around the Comm -- around the United States who has expressed some interest in Facebook and the -- in the aftermath of Cambridge Analytica.

Do I have that right?

MS. ELLSWORTH: You do.

THE COURT: Have any other courts addressed this issue about privilege or work

product?

MS. ELLSWORTH: No, your Honor. There's not -- it has not come to another...

THE COURT: I am lucky enough to be on the cutting edge?

MS. ELLSWORTH: Yes. As to -- as to the ADI, you are the first.

THE COURT: All right. Anything else?

MS. ELLSWORTH: No, your Honor. Thank you.

THE COURT: Ms. Cable, so you heard my questions for Ms. Ellsworth.

MS. CABLE: Yes.

THE COURT: Let me ask you a quick question, and then I'll give you an opportunity to respond.

One point that she makes is that prior to March -- March of 2018, when the ADI came into being, there were also elements of Facebook's enforcement program that included attorney-client communications.

So you can imagine that on occasion, for example -- and, again, and I know that I am looking at the materials that have been provided, I think it's Exhibit N, page 6, which is a letter

from Facebook to Chairman Chuck Grassley on the U.S. Senate Committee on the Judiciary says on page 6 that in 2017 -- for example, In 2017 we to ask action against about 370,000 apps ranging from imposing certain restrictions to removal of the app from the Platform.

So I can imagine that in dealing with 370,000 apps that Facebook deemed to be, perhaps, in violation of its policies; some attorney-client communications were generated.

MS. CABLE: Theoretically. I mean, I don't think I can because I just don't think we have a record here.

Part -- part of the issue here is a lack of a record, a factual record, for the Court to look at.

THE COURT: And I saw that. There is a reference, I think, that and in some of the footnotes about how we had a full -- some of the decisions that were rendered had a fuller factual record than I have here.

MS. CABLE: That's, that's true. And that's really the problem.

Because, as you've heard, the position that Facebook has taken is that because the ADI

was undertaken in anticipation of litigation and because lawyers were involved at every step of the way to varying degrees, everything related to it, no matter what, it's cloaked. That is not the law.

THE COURT: Um-hum.

MS. CABLE: The law -- I am aware of no case where underlying facts have been shielded from disclosure.

And maybe that the form in which those facts appear in the form of a communication or a lawyer memo are shielded; but a party -- the opposing party always needs to have access to some way to get to those facts.

The identity of these apps --

THE COURT: Actually, that's another holding of *Chambers*.

MS. CABLE: Right.

THE COURT: The SJC says, it does not --

MS. CABLE: It's --

THE COURT: -- immunize underlying facts.

MS. CABLE: Neither the privilege nor the work-product doctrine.

THE COURT: Got it.

MS. CABLE: This is what Facebook is

trying to do here.

I do think -- I will not dispute there are elements of the ADI that probably are protected by a work-product protection or the attorney-client privilege.

THE COURT: So how do we draw that line?

MS. CABLE: I think your Honor was right on it.

What are we seeking here? We are seeking the identity of apps that Facebook has some reason to think it violated its policies and basic information about them.

Facebook's own admissions to the public, to us, to Congress are that since 2012 they've endeavored to do that. This is an ongoing business practice.

The prospect of litigation was not the reason. It was not because of that that they are policing their Platform.

The information we are seeking is who are you policing? That's what we want. Not why. Not what did why you are attorneys say about it?

THE COURT: Who are you policing and, again, to some extent, you are focusing on and when did you become aware that perhaps they

required policing?

MS. CABLE: I don't -- I think we are saying what was the basis for?

They can respond to that saying the basis was, you know, during the ADI; and that is work product.

They can say that. That's -- that's relevant information.

THE COURT: Um-hum.

MS. CABLE: Right? Because then we know that they didn't look at this until the ADI. But we don't -- they are not willing to do that.

So if -- if I could just point the Court -- because I think part of the difficulty for me preparing, and maybe the Court struggling is, what are we talking about? I you would --

THE COURT: That's one way you could put it.

MS. CABLE: Tangibly what is this? There's been some references to that -- there's attorney-generated lists identifying these apps.

The list is not before the Court for an in-camera review.

And if you read the Chen declaration, she doesn't actually say that such lists have been

created.

So the theory is, if they were to create such a list to provide to us, that list would somehow allow us to retro engineer and back ourselves into the attorney thought processes.

One way to gauge the validity of that is to look at Exhibits PP and QQ.

THE COURT: One moment.

MS. CABLE: And these were filed under impoundment. And to make this point, if you have the unimpounded or the --

THE COURT: I do.

MS. CABLE: Okay. Great.

I have copies, too, if counsel -- you have them?

THE COURT: Well, I've got, let me see, PP -- I've got the impounded version. So I've got the full version of the exhibits.

MS. CABLE: The full -- that's exactly right. So just to --

THE COURT: So PP and QQ?

MS. CABLE: PP and QQ.

Now, these are letters from Facebook to us during the investigation. These may look familiar to you, because they came up previously.

THE COURT: Yep.

MS. CABLE: These are lists -- in the appendicis are lists of apps that Facebook has actually taken an enforcement action against.

THE COURT: Um-hum.

MS. CABLE: So by counsel's admission, this is where a real attorney has gone in and made individualized judgments.

We don't know, because we don't have the list, but I expect this is what the list would look like if your Honor rules in our favor.

If your Honor can discern any attorney thought processes from these lists, I can't -- so we can say that some aspect of the ADI is protected by work product; and we can still say that it's not because of litigation this they wanted to identify violators of their policies, but even if it was, at best, we are talking fact work product here.

There is nothing -- if the lists look like this -- and this is, again, the most clear distillation of attorneys thought processes -- they don't reveal any mental -- any opinion work product here.

THE COURT: So -- and I agree with you.

Part of what I've been wrestling with -- and we started here, which is what are you looking for?

Then we got that pesky Category 6 where the AG wants all internal communications.

So I'm looking at a list of -- goodness gracious -- how many?

Actually, I can't tell by the numbers, but it looks like several hundred apps here.

You want all the internal communications having to do with these apps?

MS. CABLE: I don't think we do. Your Honor, when we write these CIDs, I mean, this was months before -- we know a lot more now than we did then.

THE COURT: Yes.

MS. CABLE: And, again, typically there are meet and confers over the perimeters of these kinds of requests.

We simply have not had the chance to have that meet and confer because of this privilege issue.

THE COURT: So, for example, if I address this by focusing on the lists, the identification of the apps, identification of developers, and

some of the other subcategories of your requests, I think it's specifically 1, 3, and 4 -- 1, 2 and 4.

MS. CABLE: One, 2 and 4.

THE COURT: Got it. Focus on those --

MS. CABLE: Yep.

THE COURT: -- and put off a ruling with respect to 6, that's a good starting place?

MS. CABLE: It's a starting place. I think my concern would be, again, because they've taken the position that all communications related to the ADI blanket not producible because they are privileged. We obviously disagree with that. There's no factual record substantiating that.

I think at the least we would need to meet and confer; we can talk about through perimeters, but they need to justify whether or not a privilege applies. And -- and -- and --

THE COURT: But, so when I say, put off. So I would defer, perhaps, perhaps, I haven't made up my mind here yet. But I am trying to be practical about this.

So, for example, your Request No. 6 asks me to -- I've got to figure out the dividing line

between what would be legitimate attorney-client communications resulting from the ADI and what would not be legitimate.

And I'm flying blind as well. I haven't seen the documents, so I don't understand the level of attorney involvement in a particular phase, so I am having some difficulty drawing that line.

But if the starting point was we need to understand, "we" being the Attorney General's Office, we need to understand which apps fall into these various categories without -- again, no waiver -- and I want to come back to the waiver argument again in a moment -- but no waiver of any argument as to the attorney-client privilege or work product protection associated with any of those communications that would fall within Category 6.

That would be a logical starting point.

MS. CABLE: I agree, that would be a logical starting point, yes, your Honor.

THE COURT: Waiver -- you did make a waiver argument in your papers, are you pressing that?

MS. CABLE: I'm not pressing it; but I

will -- I will point out that Chapter 93A does put the burden on the party opposing the CID to take some affirmative action.

Part of the difficulty we have here is as a result of months and months of dribs and drabs of information about the ADI without giving us the actual information.

So I guess my point on waiver is just time is of the essence.

It's been a long time. We are now coming on a year since we issued the CID. We need this information.

THE COURT: I see. Well, that's why I am here. And I looked -- took a look at the *Body Metric* case, that's sort of the lead case here. If I read that case correctly, it says, it may be deemed a waiver, but it's not automatically a waiver.

I got to assume that I still have discretion on whether to determine whether -- that a waiver has taken place.

And, certainly, in *Body Metric*, it looked like they pretty much ignored --

MS. CABLE: Yeah.

THE COURT: -- the CID for a long time.

MS. CABLE: Yeah. And that's not the case here.

THE COURT: And that's not the case here.

MS. CABLE: No.

THE COURT: No. I got it. Let's of communications back and forth.

MS. CABLE: Yes.

THE COURT: Let me ask you another question, and then I'll give Ms. Ellsworth one more crack at it.

Which is, so what would a privilege log -- if I were to order a privilege log here, what would it look like?

What -- again, so, for example, if I take literally your Category 6, I don't -- I'm not sure that privilege log would fit within the City of Boston.

MS. CABLE: I don't know that I would want to receive that privilege log.

THE COURT: Again, I am assuming that's there's a lot of work that's gone on here. Every communication, every email, every text message, ever communication that's taken place in the context of the ADI with respect to -- even if we limit it to the apps that fall within those

categories, I am guessing that's a lot of information.

How do we -- how do we do that in -- by way of a privilege log?

MS. CABLE: I can't say here, your Honor. I can -- I absolutely agree, there's going to need to be discussions.

And we've -- we've sort of preliminary had those discussions just teed up the issues of what are we going to do here.

I think the first step is to understand the body of apps that we are entitled to get discovery on.

From there we can start talking about custodial limits to the emails, time limits to the emails. There's various ways to whittle down the information.

But, you know, when we draft these CIDs, we don't have any of that information, so we'd necessarily have to start broad.

THE COURT: So, for example, if I were to differ on Category 6, that would probably also mean deferral on a privilege log for the moment. For the moment. Got it. Okay.

Ms. Cable, what else do I need to know

that we haven't discussed?

MS. CABLE: I think we've discussed everything, thank you.

THE COURT: Ms. Ellsworth, back to you.

Anything else that you think I need to know?

MS. ELLSWORTH: Judge, a few things just in response to some of the points made by Ms. Cable.

On the question of whether these are just facts, we agree that just facts are not shieldable by privilege or work product, right, that's Black Letter Law.

THE COURT: So but -- so let me ask you, to hold your feet to the fire.

So there are no just facts anywhere in the ADI because you're claiming everything is privilege.

So we shake the ADI and no just facts fall out.

MS. ELLSWORTH: They could ask for something that would be just facts. The Attorney General could say, I would like a list from you of all apps that have XYZ perimeters that have -- that are from this jurisdiction that have this

many privacy sittings.

They could ask -- they could say, this is what we think, we the Attorney General --

THE COURT: Um-hum.

MS. ELLSWORTH: -- think should be suspicious or think you, Facebook, should find suspicious.

That would be information that we could -- to the extent we have it, we could generate factual information for them.

That would not be subject to the claims of privilege and work product.

What they are asking for here, and Ms. Cable just articulated it, apps that we, Facebook, we, the ADI, have found suspicious for one reason or another, which is an attorney suspicion.

That is asking for our investigation, right, and that is the major disagreement I think that we have here with the Attorney General.

They are asking to take our investigation and turn it over to them.

THE COURT: Pre-March of 2018, was it attorneys who determined what was suspicious?

MS. ELLSWORTH: Prior to 2018, there were

different things that were being considered, so I --

THE COURT: Was it in -- prior to March of 2018, did Facebook always rely upon attorneys to determine what apps were suspicious?

MS. ELLSWORTH: I don't know the answer to that question, and I'll defer to Mr. Southwell in a minute.

But I do want to continue to make the point, which I think is a valid one.

These are -- all of these lists we are talking about are lists that were generated in the ADI by attorneys, and by the involvement of attorneys, or at the direction of attorneys.

THE COURT: And I've got that point. So you -- you say -- I guess, as I take it, any time an attorney touches any of these, is it has any input either in actually categorizing or in setting any perimeters that result in categorization that's protected?

MS. ELLSWORTH: It's just like the list of employees.

THE COURT: What I said was correct?

MS. ELLSWORTH: Yes. It's pro -- it's all protected.

And it's just like the list -- by the attorney-client privilege and the work-product doctrine, we think they are coextensive here for the reasons that we've articulated.

THE COURT: Got it.

MS. ELLSWORTH: But it's just like the list of employees that are interviewed in an internal investigation.

Those are not permitted to be turned over.

The information that the adversary can get or the regulator can get are employees who you think might have information, right.

Those are different questions. Whether they generate the same response, nobody knows.

But that's the type of factual information the Attorney General would be entitled to and they could have asked for and can still ask for.

And that's not what we are dealing with here.

THE COURT: Yeah. If it was a company policy, I think every workplace accident result in interviews of the people who were present at the time of the accident.

Not conducted by attorneys. Conducted by health and safety.

And then they have a really bad accident, so they bring attorneys in to conduct the interviews.

Are you saying that all the prior interviews, the ones that weren't conducted by attorneys, that's all protected? Same? Are you saying --

MS. ELLSWORTH: I'm not sure I understand the hypothetical. But I don't even think we would say in that circumstance that the attorney-conducted interviews -- there would be facts in those interviews that would -- that would not be protected by the privilege or the rules.

THE COURT: So the interviews themselves, though, you would say would be protected?

MS. ELLSWORTH: Well...

THE COURT: An attorney-conducted investigation of a workplace accident, you say --

MS. ELLSWORTH: You mean the identity of the employees?

THE COURT: Not -- no, no. And I've got Upjohn. I know Upjohn. I got the identity of

the employees. But we are talking about -- in Upjohn, they were fighting about the actual interviews.

MS. ELLSWORTH: Right.

THE COURT: So are you saying that -- again, your position is the attorney conducted interviews, they are protected. Right?

MS. ELLSWORTH: If they are conducted for purposes of rendering legal advice.

THE COURT: Yes. But if I understand -- if I understand your position as well, you are saying that somehow that's -- again, I guess my point is simply, those investigations can be undertaken outside the scope of the privilege and outside the scope of work-product protection in other circumstances by, for example, company employees, right?

So, for example, if the employees -- if an employee from the Health and Safety Department does investigations of a workplace accident with no attorney involvement, that's not protected, right?

MS. ELLSWORTH: That's correct. But that wouldn't -- that investigation wouldn't involve the attorney judgment and the attorney legal

advice that an attorney-lead investigation would, right?

That's the difference, and we think it's an important one.

I would also note that Ms. Cable pointed to Exhibit PP as an exhibit of the type of lists --

THE COURT: Yes.

MS. ELLSWORTH: -- that she thinks might be generated.

THE COURT: Yes.

MS. ELLSWORTH: Again, looking at request No. 2 and all of the types of information surrounding the identification of apps that the CID calls for, it's much, much, much more than what you see in the impounded version of the attachment to PP, right, it's the basis and the initial source of the concerns of misuse.

There's a lot more information that they're seeking; and that information is, again, the attorney-generated information and the suspicion.

As to the privilege log, I think we've sort of dealt with that. Not just -- not only would it be incredibly burdensome to do a

privilege log -- I would note, and we have given these numbers both to the Attorney General's Office and, I think, to the Court.

THE COURT: Um-hum.

MS. ELLSWORTH: They are aware of the number of apps we are talking about here is in the millions range, so not just burdensome and unwieldy but simply undoable.

So that's --

THE COURT: Yeah. That is a function at some level of the position that Facebook is taking, which is everything is protected.

So everything would have to be on the privilege log.

MS. ELLSWORTH: I think it is a function of the breadth of the request, your Honor. It particularly requests this.

THE COURT: Well, yes, they are asking for information about the ADI.

And your position is everything that the ADI does is protected?

MS. ELLSWORTH: Our position is that this CID is the equivalent of asking for a company's privileged internal investigation.

THE COURT: Right. I've got that.

What else do I need to know?

MS. ELLSWORTH: That's it, your Honor, I think.

THE COURT: All right. Ms. Cable, very briefly. Yes?

MS. CABLE: Yes, just to respond. Ms. Ellsworth suggested that we could have asked -- phrased our CID as asking for particular categories that we came up with.

I just want to point out, we sought information prior to the CID.

We asked Facebook, before we even knew anything about the ADI, tell us the apps that you've taken some enforcement action against short of suspending them.

And this is Exhibit NN, our second CID. They said no. They said, We can give you information prior to March 2018, but everything past that is ADI and it's protected. And they wanted us -- and they just refused.

And in order to move the issue forward, we asked, Can you describe the ADI to us, because we're not convinced?

And that's what prompted months of the back-and-forth descriptions.

Finally, we said, we are going to do a third CID using your description of the ADI to try to tell you what we are looking for.

So it is -- for them to say we are trying to dig into the ADI, they led us right there.

And so -- and you can see there's a -- I think, a little bit of gamesmanship going on here.

THE COURT: Um-hum.

MS. CABLE: The point is, they are refusing to provide this information, and we think it's factual. We don't think this particular information is covered.

So I just want to point the larger context out.

THE COURT: Well, if I understand Facebook's position at some level, it's figure it out for yourself. That's the position.

So -- all right. Here's what I'm going to do. I need to take some time and think about this one.

I understand this is an urgent matter. I'll try to get you something as soon as I can.

I -- honestly folks, I have a fair number of urgent matters before me. So this will be in

the queue. I will attempt to address it, again, as quickly as I can. I try to be practical about this stuff.

And you've heard my questions. You've heard -- I think I've staked out some positions on at least what I think the cases stand for today.

I have to say, I have some concerns about the extent of the work product and attorney client claims here.

And so I am going to take a further look at it, but I am going to churn out a decision as quickly as I can.

Do you have a next date in this? Do we need a next day?

This is not your average case in the sense that this is a petition to enforce the CID. I -- I don't know whether it makes sense for us to have a next date.

Let me ask, Ms. Cable, what do you think?

MS. CABLE: I think it may make sense to, subject to the Court's schedule, set maybe a status conference.

In particular, I am thinking in light of what we discussed, if the Court rules in our

favor on Requests 1, 2, and 3 and defers on 6, we may need to come back for some clarification through our meet and confers.

I would be in favor of just having something on the calendar. We can take it off if we don't need it, but...

THE COURT: So here's one of the issues that we face in the session. I'm in the session half of the year. I am not in the session for the entire year.

MS. CABLE: Right.

THE COURT: So I will be leaving the session at the end of December. I don't know exactly where I am going, hopefully, I will stay within the Commonwealth of Mass. if I've been good. So that's the plan.

But I won't be in BLS 1. And this case has not been specially assigned to me.

All right. So what I am going to do, it seems to me, that I need to make -- render a decision that it may leave open some issues that have to be resolved going forward.

I am not saying -- I can't guaranty that I will be the one that resolves those.

MS. CABLE: Understood.

THE COURT: It makes sense for you, I suppose, to come back to me, if necessary, for clarification on a particular holding that I make, a ruling that I make.

But if there are additional rulings that are required in the aftermath of my initial rulings, those don't necessarily have to come from me.

And there are very capable judges who will sit here.

I think your next judge is going to be Judge Green.

So they are very -- Judge Green is very capable and so, it may be -- the appropriate route may be to -- any additional matters that have to be resolved in the case would then be resolved by Judge Green.

So, Ms. Ellsworth?

MS. ELLSWORTH: Your Honor, just to flag for the Court.

THE COURT: Oh, no.

MS. ELLSWORTH: Judge Green will not be able to sit on this case.

THE COURT: Oh, my goodness. I thought -- just thought about that. She was at

Hale and Dorr.

MS. ELLSWORTH: Right.

THE COURT: And does she -- but you are not Hale and Dorr any more.

MS. ELLSWORTH: She was at Wilmer Cutler Pickering Hale and Dorr until about 18 months ago. So, I don't --

THE COURT: Oh, Lord.

MS. ELLSWORTH: I'd love to appear in front of Judge Green, though.

THE COURT: And is her position, as far as you know, that she takes no matters from your firm?

MS. ELLSWORTH: Yes. At least as of right now.

THE COURT: All right. Well...

MS. ELLSWORTH: I don't mean to inject further complications.

THE COURT: No, no, it's not complication. Yeah. Thank you for flagging that. That's something I hadn't focused on.

When you stood up, the first thing it did suddenly cross my mind that maybe we have recusal issue here.

And I don't know how that will be

addressed.

MS. CABLE: Sure.

THE COURT: I don't know how that will be addressed. All right.

That's something I suppose I have to get me chief involved in as well as how this case will be handled when Judge Green is sitting in BLS 1.

Sometimes we just send you off to BLS 2. So -- but we'll see.

All right. So what I am going to do is try to get my decision out to you as quickly as possible.

Anything else that we need -- so I think a date on the calendar probably doesn't make sense, okay.

MS. CABLE: Okay.

THE COURT: When I issue a decision, I'll give you a next date because I expect that there will have to be some discussion with the judge over what happens regardless of what I do.

I can't say, honestly, that I've had one of these petitions for enforcement sort of come to fruition before -- I've had them I think filed, but they always seem to get resolved in

advance.

So I'm going to -- I'm not going to give you a date right now. A date will come down with whatever order I issue.

And I'll give you some instruction in that as well as to who will be hearing on the next date.

Is there anything else that we can accomplish in this case today?

MS. CABLE: No.

MS. ELLSWORTH: I don't think so. Thank you for your time, your Honor.

MS. CABLE: Thank you very much.

THE COURT: Thank you, counsel.

MR. SOUTHWELL: Thank you, your Honor.

THE COURT: And you are free to go. It's going to take me a couple minutes to collect my papers.

(3:25 p.m. court in recess.)

The Commonwealth of Massachusetts
OFFICE OF COURT MANAGEMENT, Transcription Services

AUDIO ASSESSMENT FORM

For court transcribers: *Complete this assessment form for each volume of transcript produced, and include it at the back of every original and copy transcript with the certificate page, word index, and CD PDF transcript.*

TODAY'S DATE: 11/12/2019 **TRANSCRIBER NAME:** Lisa Phipps

CASE NAME: AGO v. FACEBOOK, INC. **DOCKET NUMBER:** 1984CV02597

RECORDING DATE: 11/7/2019 **TRANSCRIPT VOLUME:** 1 OF 1

(Circle one) TYPE: CD TAPE QUALITY: EXCELLENT (GOOD) FAIR POOR

(Circle all that apply) ISSUES (include time stamp):

background noise	time stamp:_____
low audio X	_____
low audio at sidebar	_____
simultaneous speech X	_____
speaking away of microphone X	_____
other:_____	time stamp:_____
_____	_____
_____	_____
_____	_____

COMMENTS: No log notes, spellings, or speaker IDs provided.

C E R T I F I C A T E

I, LISA MARIE PHIPPS, AN APPROVED COURT TRANSCRIBER, DO HEREBY CERTIFY THAT THE FOREGOING IS A TRUE AND ACCURATE TRANSCRIPT FROM THE AUDIO RECORDING PROVIDED TO ME OF THE PROCEEDINGS IN THE MATTER OF ATTORNEY GENERAL'S OFFICE V. FACEBOOK, INC. HELD ON NOVEMBER 7, 2019

I, LISA MARIE PHIPPS, FURTHER CERTIFY THAT THE FOREGOING IS IN COMPLIANCE WITH THE ADMINISTRATIVE OFFICE OF THE TRIAL COURT DIRECTIVE ON TRANSCRIPT FORMAT.

I, LISA MARIE PHIPPS, FURTHER CERTIFY THAT I NEITHER AM COUNSEL FOR, RELATED TO, NOR EMPLOYED BY ANY OF THE PARTIES TO THE ACTION IN WHICH THIS HEARING WAS TAKEN, AND FURTHER THAT I AM NOT FINANCIALLY NOR OTHERWISE INTERESTED IN THE OUTCOME OF THE ACTION.

Lisa Marie Phipps
NAME OF THE APPROVED COURT TRANSCRIBER
PROCEEDINGS RECORDED BY FTR AUDIO RECORDING
TRANSCRIPT PRODUCED STENOGRAPHICALLY FROM COMPUTER

November 12, 2019
DATE

LMP Court Reporting
347 Eliot Street
Ashland, Massachusetts 01721
BUSINESS ADDRESS

(508) 641-5801
BUSINESS TELEPHONE

lmpreporting@gmail.com
EMAIL ADDRESS

MASSACHUSETTS RULE OF APPELLATE PROCEDURE 16(K) CERTIFICATION

I hereby certify that, to the best of my knowledge, that this brief complies with the Massachusetts Rules of Appellate Procedure that pertain to the filing of briefs. The brief is in the Times New Roman font, with a text size of 14 point, and headings in either 14 or 16 point as provided in Mass. R. App. P. 20(a)(4)(B). The brief was composed in Microsoft Word, version 1902, build 11328.20230, and the portions of the brief subject to length limitation, as provided in Mass. R. App. P. 11(b) contain 1,950 words based upon the word count provided by that software.

/s/ Felicia H. Ellsworth
FELICIA H. ELLSWORTH
(BBO # 665232)
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Felicia.Ellsworth@wilmerhale.com

April 15, 2020

CERTIFICATE OF SERVICE

I, Felicia H. Ellsworth, hereby certify, under the penalties of perjury that on April 15, 2020, I caused a true and accurate copy of the foregoing to be filed via the Massachusetts Odyssey File & Serve site and in the office of the clerk of the Supreme Judicial Court and upon the following counsel by electronic mail:

Sara E. Cable, Esq.
Peter N. Downing, Esq.
Jared Rinehimer, Esq.
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
(617) 727-2200

/s/ Felicia H. Ellsworth

FELICIA H. ELLSWORTH
(BBO # 665232)
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Felicia.Ellsworth@wilmerhale.com