No. SJC-12946

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

BRIEF FOR RESPONDENT-APPELLANT FACEBOOK, INC.

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

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

July 27, 2020 *Attorneys for Respondent-Appellant Facebook, Inc.*

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

Page(s)

STATUTES AND RULES

INTRODUCTION

In March 2018, several media outlets broke the news that a company called Cambridge Analytica had misappropriated Facebook user data. Given the nature of the news, Facebook anticipated that it soon would face litigation arising from this event. It was right. Within days, Facebook was sued, and within several weeks, it was facing dozens of lawsuits and regulatory inquiries across the country. To prepare for this anticipated and actual litigation, Facebook—like companies do every day—hired outside counsel to conduct an internal investigation and advise the company on its litigation risks and strategy. In so doing, Facebook relied on the well-established protections for such legal investigations articulated by seminal cases like *Upjohn Co. v. United States*, 449 U.S. 383 (1981) and *Commissioner of Revenue v. Comcast Corp.*, 453 Mass. 293 (2009).

Consistent with these well-settled principles, Facebook's internal investigation, commonly referred to as the App Developer Investigation ("ADI" or the "Investigation"), mirrors the confidential investigations that companies routinely conduct to obtain legal advice, and that courts routinely find protected by the attorney-client privilege and attorney work product doctrine. Facebook's legal counsel, operating with an eye towards litigation, developed a protocol for analyzing historic activity on Facebook's Platform to determine Facebook's legal risks and to respond to potential and actual litigation. Counsel operated separately

from other groups at Facebook and maintained strict confidentiality over their investigative processes and efforts. And they worked towards a quintessentially legal goal: to address and react to Facebook's litigation exposure arising from any other bad actors who (like Cambridge Analytica) may have misused data before Facebook put additional safeguards into place in 2014.

The Attorney General is also interested in whether other bad actors may have misused data obtained from Facebook users. That is her prerogative, and she has the right to pursue it. But the central question in this appeal is whether, in pursuit of her own investigation, the Attorney General can bypass the normal course and commandeer the fruits of an attorney-driven investigation commenced in response to actual and anticipated litigation—which is precisely what the Superior Court's order would allow her to do. The Civil Investigative Demand before this Court copies, verbatim, the structure and terminology of Facebook's Investigation, including, critically, those portions that expressly describe choices made by Facebook's counsel in designing and undertaking the Investigation. Instead of devising her own investigative criteria, the Attorney General has sought to piggyback on the work of Facebook's counsel—and has done so in terms that call for the disclosure of material that is inherently protected by the attorney-client privilege and work product doctrine. In effect, the Attorney General asks Facebook to divulge the identity of and information about every application

("app") Facebook's attorneys chose to investigate (and every communication about those apps).

That is not permitted. In our adversarial system, litigants cannot bypass the limits of discovery and instead demand the fruits of their opponent's labor; that is precisely what the long-standing laws of privilege and work product are designed to prevent. The chilling effect of any rule to the contrary cannot be overstated. This Court should reverse the Superior Court's outlier decision.

STATEMENT OF ISSUES PRESENTED FOR REVIEW

1. Whether a company can be compelled to produce information and communications generated as 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 can be compelled to produce information created pursuant to a lawyer-developed internal investigation in anticipation of litigation, simply because that company also employs routine non-legal enforcement of its policies in other contexts.

STATEMENT OF THE CASE

On November 5, 2018, the Massachusetts Attorney General issued a Civil Investigative Demand ("CID") to Facebook pursuant to Mass. Gen. Laws c. 93A,

§ 6. A1/53-73.[1] Facebook complied with the CID except to the extent it calls for Facebook to produce information protected by the attorney-client privilege and work product doctrine. As to those portions of the CID, Facebook promptly identified its objections to the Attorney General and confirmed it would not waive the attorney-client privilege or the protections of the work product doctrine. *See, e.g.*, A1/454-461; IA151-158.

On August 15, 2019, the Attorney General filed a Petition to Compel Compliance with the CID. A1/20-52; IA8-41. On January 16, 2020, the Superior Court granted the Petition in part and ordered compliance with the Order within 90 days.[2] A2/178-196.

Facebook noticed its appeal on February 4, 2020. A2/197-198. The appeal was docketed in the Appeals Court on March 19, 2020. Facebook filed an application for Direct Appellate Review on April 15, 2020, and this Court granted the application on May 13, 2020.

---

[1] References to "A" refer to the appendix filed herewith; references to "IA" refer to the impounded appendix.

[2] On March 2, 2020, the Superior Court denied Facebook's request for a stay of the Order pending appeal, and, on March 30, 2020, a single justice of the Appeals Court did the same. The parties entered into a protective order governing the treatment of materials Facebook produced during the pendency of this appeal. Facebook has been producing materials to the Attorney General on a rolling basis since April 15, 2020, subject to Facebook's right to claw back those documents if the Order is overturned on appeal.

STATEMENT OF FACTS

A. The Facebook Platform

Facebook offers an online social networking service that enables people to connect and share information with their friends, family, and communities. In 2007, Facebook launched an additional service called the Facebook Platform (the "Platform"). A1/222. The Platform empowers users to share Facebook data with apps as well as app developers so that users can experience the internet and social media in new and interesting ways. Specifically, the Platform allows third-party app developers to integrate certain Facebook technologies into their own apps—for example, a third-party developer could use the Platform to enable a calendar app to import a user's friends' birthdays into a single, convenient place. Further, the Platform makes life easier for Facebook users by letting them log into other services and apps using their Facebook credentials. A1/341. And, via the Platform, users can connect with their Facebook friends on third-party services by, for example, seeing those friends' housing or cooking recommendations on popular apps like Airbnb or Pinterest. This dynamic interaction fosters connections and fuels innovation that might not otherwise be possible.

The Platform is and has been governed by a robust set of policies that prohibit developers from selling or otherwise monetizing Facebook user data, or transferring data to third parties without a Facebook user's consent. A1/222-223.

Facebook's policies also empower users to control their own data—and, importantly, only permit access to users' data to the extent allowed by users' own privacy settings (which users can control). A1/217; A1/222.

In 2014, Facebook launched a series of additional data privacy protections on the Platform. A1/105-112. These changes included additional, significant limitations on the amount of data that developers could request from Facebook users, limitations on the data about users' friends that developers could access, and more granular control for users over what information they shared with apps. A1/217.

B. The Media Reports on Data Abuse by Cambridge Analytica

In November 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app on the Platform called "thisisyourdigitallife." A1/221. Consistent with the pre-2014 Facebook Platform policies, Facebook users who logged into Kogan's app gave their consent for Kogan to access information they shared on Facebook, as well as information about their friends, but *only* to the extent permitted by those friends' privacy settings. A1/222.

In December 2015, *The Guardian* published an article reporting that Cambridge Analytica, a British political consulting firm, used Facebook data collected by Kogan to create "psychographic profiles" to support its political consulting work. A1/230. Although Kogan and Cambridge Analytica initially

denied any misappropriation of Facebook user data, Facebook nonetheless took immediate action. A1/230-231. It banned Kogan's app, and then secured certifications from Kogan, Cambridge Analytica, and related entities, that they had deleted all user data that they had misappropriated. A1/230-231.

In March 2018, several news organizations, including *The New York Times* and *The Guardian*, reported that the data Kogan and Cambridge Analytica misappropriated may not, in fact, have been deleted—contrary to Kogan's and Cambridge Analytica's certifications. Facebook again took immediate action. It banned Cambridge Analytica, Kogan, and related parties from the Platform and began investigating the degree to which Kogan and Cambridge Analytica violated their certifications. A1/232.

C. Facebook Launches the App Developer Investigation

1. Facebook Hires Outside Counsel to Design and Run an Investigation

Facebook anticipated an array of legal challenges arising from the Cambridge Analytica incident and surrounding media attention. A2/48-49 (¶ 4). Indeed, a wave of litigations and regulatory investigations immediately followed. In addition to this case, at least sixty-five other litigations relating to the Cambridge Analytica events have been filed against Facebook since March 2018, including securities class actions, derivative actions, books-and-records actions, consumer-based suits, and suits by developers. Facebook also has received

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. A2/54-55 (¶ 22); A2/62-66.

In order to respond to these actual and anticipated legal challenges, Facebook understood it would need legal advice and counsel. A2/48-49 (¶¶ 4-5). To that end, Facebook initiated a legally driven internal investigation into developers and apps that, like Kogan and his app, were active before Facebook's 2014 Platform changes and may have had access to large amounts of user data. *Id.* Facebook had never conducted an internal investigation of this nature and historical scope,[3] and there existed no standard company, or even industry, template or practice for how such an investigation should be designed or implemented. A2/49-51 (¶¶ 5-8). Thus, Facebook hired outside counsel (Gibson, Dunn & Crutcher LLP) with extensive experience in conducting cybersecurity and data privacy internal investigations to design and direct this new investigation. *Id.*

[3] As explained *infra* 20-21, 45-46, Facebook's routine enforcement mechanisms were neither designed to nor capable of conducting the backwards-looking legal review Facebook needed, and thus Facebook's counsel designed a review that would address the specific legal problems presented.

Facebook intentionally structured the Investigation as a confidential, internal, retrospective, and legal-driven review. Specifically, Facebook's counsel designed the Investigation primarily to review apps that were active *before* Facebook's 2014 Platform changes, with the core purpose of uncovering and assessing legal risks posed by those apps and providing legal advice to Facebook about litigation, regulatory inquiries, and other legal challenges facing the company. A2/50 (¶ 7).

Further, Facebook's counsel managed and have overseen all stages of the Investigation. A2/50-51 (¶ 8). For example, 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 investigations. A2/51 (¶ 9). Working with these forensic consulting firms, Gibson Dunn and Facebook's internal counsel developed an investigative framework that reflected their assessment of which types of apps pose the greatest legal risks, how Facebook should prioritize its review in light of potential legal risks, and when Facebook should pursue further action, including litigation. A2/51 (¶ 11). And, Facebook's counsel have taken steps to ensure that communications by and among individuals working on the Investigation remain confidential and privileged, including by limiting communications about the Investigation and restricting access to investigatory documents.

Consistent with its legal purpose, the Investigation has informed Facebook's legal decision-making. A2/54-55 (¶¶ 22-23). Facebook's counsel have used information generated in the Investigation to advise the company about how to respond to litigations and mitigate legal risk, including in litigation commenced by Kogan. A2/54-55 (¶ 22). Further, Facebook's counsel have used information generated in the Investigation to pursue offensive litigation. A2/55 (¶ 23).

Given the highly publicized nature of the Cambridge Analytica events, and consistent with Facebook's commitment to transparency, Facebook has made occasional generalized public statements about the Investigation's creation and goals. *See, e.g.*, A1/327-329; A1/330-334; A1/335-338. For example, on March 21, 2018, Facebook's founder Mark Zuckerberg publicly announced the Investigation, explained its purpose as "investigat[ing] all apps that had access to large amounts of information before we changed our platform to dramatically reduce data access in 2014," and also stated that the company would inform users if their personal data is found to have been abused. A1/327-329; *see also* A1/330-334. A month later, Facebook similarly responded to congressional inquiries by explaining that it was investigating apps "that had access to a large amount of information before we locked down our platform," and stated that, "if we find that someone is improperly using data, we'll ban them and tell everyone affected." A1/342. And in May 2018, Facebook again stated that it was conducting a

"comprehensive review to identify every app that had access to [pre-2014 Platform] data," and that it would tell users if their data was abused before the 2014 changes. A1/335-338. Facebook updated its community again in September 2019, reaffirming its prior commitments and providing some high-level information on the Investigation's status to-date. A2/70-73.

2. The Investigation Is Separate and Distinct from Facebook's Other Enforcement Efforts

Consistent with its unique litigation purposes, the Investigation is radically different than Facebook's preexisting monitoring, compliance, and enforcement efforts. Facebook's routine policing of the Platform is conducted by a team known as Developer Operations, or "DevOps." A1/176-177; IA/46-47. The DevOps team monitors, in real time, daily app and developer behavior on the Platform with the aim of identifying abnormalities that might signal potential policy violations. A1/177-178; IA47-48. DevOps also enforces Facebook policies, and has developed its own rubrics and procedures for how to enforce those policies against bad actors. A1/178-179; IA48-49. In some instances, DevOps may elevate a particular question or suspected abuse to Facebook's lawyers for further guidance, but generally DevOps is not a legal-supervised effort. A178-179; IA48-49.[4]

[4] The specific details of DevOps rubrics and ongoing enforcement are confidential and can be found in the impounded appendix at IA43-59.

By contrast, the Investigation—launched specifically in anticipation of the dozens of litigations that immediately followed the 2018 media reports—is not a routine, daily, or real-time policy monitoring team. A2/49 (¶ 5). The Investigation is retrospective, focused on apps and developers with access to large sets of user data before the 2014 Platform changes. A2/50 (¶ 7). Unlike DevOps, which is operated contemporaneously with the current Facebook Platform, the Investigation is focused on the potential legal risks of a finite, albeit large, number of apps and developers that primarily were active on a now-obsolete version of the Platform. A2/49-50 (¶¶ 5-7). Further, unlike DevOps, which operates under the guidance of non-lawyer Facebook employees, the Investigation is and always has been an attorney-led investigation—outside and in-house attorneys designed, and have overseen, the Investigation from its inception. A2/50 (¶ 8). Indeed, the Investigation was established specifically *because* the DevOps team could not (i) address Facebook's legal risks with respect to an historical Platform, (ii) address compliance risks with applicable laws on an historical Platform, or (iii) assess Facebook's position in anticipated litigation and regulatory inquiries. A2/49 (¶ 5); A2/50-51 (¶ 8); A2/54 (¶ 22).

3. The Investigation's Three-Phase Design

Facebook's internal counsel and Gibson Dunn, along with the technical experts working under Gibson Dunn's direction, devised a three-phase

investigative strategy to address legal risk posed by apps and developers that may have had access to large amounts of user data before the 2014 Platform changes. These phases—which are unique to the Investigation and distinct from DevOps—are: (i) Detection and Identification, (ii) Enhanced Examination, and (iii) Enforcement. A2/51 (¶ 11); A1/476-477; IA166-167.[5]

The first phase—Detection and Identification—involves analysis of apps using four risk-based approaches operating according to criteria and methodologies designed by counsel. A2/51-52 (¶ 12); A1/476; IA166. These four methodologies include the user-impact and categorical methods, in which counsel-developed thresholds are used to cull apps posing potential legal risk; the escalations method, in which counsel identify which *ad hoc* escalations warrant legal-led review; and the low-impact method, in which counsel-selected criteria are employed to *deescalate* apps posing less legal risk. A2/52-53 (¶¶ 13-16); A1/476-477; IA166-167.

The second phase is "Enhanced Examination." A2/53 (¶ 17); A1/478; IA168. Here, Facebook's counsel directs the Investigation's forensics teams to conduct "background" and/or "technical" investigations of certain apps identified in the Detection and Identification phase, and requests detailed technical reports

[5] More granular details about the structure of the Investigation are confidential and can be found in the impounded appendix at IA162-170.

for review by outside counsel. A2/53 (¶ 17); IA168; A1/478. Counsel also employs a data-driven "risk prioritization model," developed by counsel for purposes of triaging which apps should be elevated to Enhanced Examination. A2/53 (¶ 18); A1/478; IA168.

The third phase of the Investigation is "Enforcement," in which counsel direct Facebook's engagement with the potentially offending app or developer and make case-by-case determinations of what enforcement actions are appropriate (such as cease and desist letters or litigation). A2/53 (¶ 18); A1/478-479; IA168-169. Facebook has suspended tens of thousands of apps based on legal advice obtained via the Investigation. *See, e.g.*, A1/380-386; A1/391-402; IA107-113; IA118-129.

D. The Attorney General Seeks the Fruits of Facebook's Investigation

The Attorney General commenced an investigation into the Cambridge Analytica events in March 2018. To date, she has issued three CIDs, and Facebook has cooperated with each of them. For example, in response to the first two CIDs, Facebook produced over 30,000 documents across more than 17 productions. Facebook also provided the Attorney General with numerous briefings concerning its privacy and data security policies, including briefings in which Facebook described—expressly without waiving any privilege protections—

the steps it was undertaking in the Investigation to ascertain whether any additional data abuse had transpired. A1/473-474; IA163-164.

The Attorney General's third CID (at issue here) is targeted specifically at the Investigation. Unlike the prior two CIDs, the third CID seeks information Facebook's counsel generated during the Investigation, borrowing verbatim from the information Facebook supplied to the Attorney General about the Investigation in various briefings. To the extent the third CID calls for non-privileged information, Facebook has produced the information requested. A1/63-64; A1/473-475; IA163-165. For example, because Facebook claims no privilege over communications with third parties or enforcement actions taken against third parties as part of the Investigation, Facebook promptly complied with requests seeking that information and identified apps that engaged in "actual misuse" and were banned from Facebook as a result. A1/474-475; IA164-165. Facebook also identified third-party developers that it sought to interview or audit or to which it sent an information request, and Facebook produced responsive communications with developers, as well as information about apps Facebook suspended as a result of the Investigation. A1/474-475; IA164-165.[6] In total, both before and in

[6] As Facebook has repeatedly informed the Attorney General, the mere fact of an app's suspension does not indicate that actual data misuse occurred—often, apps have been suspended because the developer failed to respond or cooperate with

response to the third CID, Facebook has produced over 16,500 pages of information across seven productions, provided detailed non-privileged information over eight in-person and telephonic briefings, and made ten narrative submissions containing detailed information. A1/474-475; IA164-165.

The aspects of the third CID at issue in this litigation are those that specifically target the internal attorney-created and attorney-led processes of the Investigation, rather than any non-privileged external output or communication. A1/63-64. Specifically, at issue in this appeal are a small subset of requests in the third CID that the Superior Court grouped into six "Contested Requests." A2/185-186; A2/196.

The first five Contested Requests share a common characteristic: each calls for the group of apps selected for investigation by the Facebook lawyers running the Investigation. A2/185-186. These groups of apps do not reflect the Attorney General's own criteria. Rather, each "group" called for by Contested Requests 1-5 corresponds exactly to apps that Gibson Dunn and Facebook's internal counsel identified and selected for review in the Investigation in order to assess potential legal risk to Facebook. *See supra* 21-23; A2/185-186. Indeed, the Attorney General copied these requests verbatim from Facebook's own explanations of the

---

Facebook's requests for information during the Investigation, and some apps were unsuspended following further investigation or subsequent cooperation.

Investigation's process. A1/53-73.[7] The first five Contested Requests therefore intentionally piggyback on Facebook's attorney-led internal investigation and nothing else. In other words, by their very design, Contested Requests 1-5 call for inherently protected materials.

The sixth Contested Request seeks all internal communications at Facebook about each of the nearly two million apps identified in the Investigation, including communications with Gibson Dunn, Facebook's internal counsel, and the consultants hired by Gibson Dunn to conduct technical analyses.

The Superior Court overruled Facebook's privilege and work product objections, giving Facebook 90 days to comply with Contested Requests 1 through 5 and to produce the communications sought by Contested Request 6, along with any corresponding privilege log. A2/196.

STANDARD OF REVIEW

This Court reviews the Superior Court's Order, which contains "rulings on questions of law," de novo. *Commissioner of Revenue v. Comcast Corp.*, 453 Mass. 293, 302 (2009). "Where, as here, we are dealing with a motion to compel

[7] In particular, the Attorney General culled language from Facebook's own descriptions of the Investigation, and used that language to target her CID. The Superior Court's Order accordingly describes the "Contested Requests" in terms of Exhibits UU and TT, both of which are narrative explanations Facebook provided to the Attorney General. *See* A1/469-471; A1/472-480; IA159-161; IA162-170.

and the motion judge's findings are based solely on documentary evidence, [this Court] does not accord them any special deference." *Id.*

SUMMARY OF THE ARGUMENT

The Superior Court's reasoning as to the attorney-client privilege errs in two separate respects. *First*, the Superior Court erroneously found two generic public statements Facebook made about the purpose and status of the Investigation to somehow vitiate Facebook's privilege (either by preventing the privilege from attaching in the first place or by waiving the privilege after it attached). *Infra* 30-37. But Facebook's public statements merely described the Investigation at a high level, and Facebook has never used the Investigation as a "sword" in this litigation, as is required to find waiver. *Infra* 33-34. As such, this Court's precedents squarely foreclose the Superior Court's finding that merely disclosing the basic contours of a privileged investigation destroys the privilege. *Infra* 34-37.

Second, the Superior Court erroneously concluded that communications that are "factual in nature" cannot be privileged. *Infra* 37-38. This Court's precedent is squarely to the contrary, acknowledging the reality that fact-gathering is an essential component of rendering legal advice and that factual communications are privileged if made for the purpose of obtaining legal advice. *Infra* 38-40. Here, as the Superior Court recognized, Facebook launched 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." A2/183. *Infra* 39-40.

The Superior Court's work product analysis is similarly flawed. *First*, the Superior Court erred by concluding that Facebook's internal investigation cannot be protected because Facebook had a preexisting, non-legal enforcement program. *Infra* 40-42. Such reasoning squarely contradicts the reasoning of this and other courts recognizing that the exception to the work product doctrine for information that would have been generated "irrespective of litigation" is exceedingly narrow, in order not to swallow the rule. *Infra* 42-46. A holding that Facebook's Investigation would have occurred as it did regardless of the litigation spawned by the well-publicized Cambridge Analytica incident contradicts the record, reality, and common sense—and disincentivizes sound corporate practice. *Infra* 42-46. The record shows the Investigation was a new and different endeavor led by attorneys to tackle a new and different legal problem, and the Superior Court's speculation cannot supplant that reality. *Infra* 45-46.

Second, the Superior Court resurrected a legal test this Court long ago put to rest, crediting the Attorney General's argument that the Investigation cannot be protected because litigation was not its "primary" purpose; but what matters is whether the Investigation was commenced "because of" anticipated litigation. *Infra* 46-49. And here again, as the Superior Court expressly recognized, the

record unequivocally demonstrates that Facebook launched the Investigation "to provide legal advice to Facebook about litigation." A2/195. *Infra* 46-49.

Finally, by parroting Facebook's own investigative mechanisms and procedures in crafting her CID, the Attorney General's requests call for documents and information that are, definitionally, opinion work product. *Infra* 49-53. Indeed, the CID uses Facebook's own Investigation against the company by repeating the terminology its attorneys developed to render legal advice and then issuing a demand for the fruits of that labor, which necessarily reflects counsel's mental impressions. *Infra* 49-53. This is exactly what the work product doctrine aims to prevent.

ARGUMENT

I. THE ATTORNEY-CLIENT PRIVILEGE SHIELDS FROM DISCLOSURE CONFIDENTIAL ATTORNEY INVESTIGATION DOCUMENTS

This Court has expressly recognized that, "[i]n a society that covets the rule of law," an "essential function" of 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." *Suffolk Constr. Co. v. Division of Capital Asset Mgmt.*, 449 Mass. 444, 449 (2007). For that "essential function" of the privilege to be served, however, "the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected." *RFF Family P'ship*,

LP v. Burns & Levinson, LLP, 465 Mass. 702, 708 (2013) (quoting *Upjohn Co. v. United States*, 449 U.S. 383, 393 (1981)).

The Superior Court's ruling injects significant uncertainty into the law of privilege for corporate internal investigations. *First*, the Superior Court found that Facebook's general public statements about the Investigation nullified attorney-client privilege protections over the Investigation, notwithstanding that the disclosures on which the Superior Court relied are generic, high-level statements about the existence of the Investigation; the Investigation does not concern activities subject to mandated reporting obligations; and Facebook has never sought to use the Investigation as a "sword" in this action. *Second*, the Superior Court concluded that certain Investigation materials and information are not protected by the attorney-client privilege because they are "factual in nature." Both conclusions are wrong.

A. Facebook's Public Statements Do Not Vitiate Privilege Over the Investigation

In reliance on a single case—*In re Grand Jury Investigation*, 437 Mass. 340 (2002)—the Superior Court found that "the materials and information called for in Contested Requests 1 through 5 … are not protected from disclosure by the attorney-client privilege because they … 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.'" A2/195 (quoting *In re Grand Jury Investigation*,

437 Mass. at 354). The Order's reasoning on this front is ambiguous at best: it is unclear whether the Superior Court concluded that, based on the two public statements the court identified, (i) privilege never attached to the Investigation because the necessary element of confidentiality was lacking, or (ii) after privilege attached to the Investigation, Facebook forfeited it through waiver. Either way, the Order misconstrues this Court's precedent and, if left undisturbed, creates the perverse result that merely disclosing the general contours of an internal investigation might eliminate privilege over confidential communications made during the course of that investigation.

1. The Investigation Is Protected by the Attorney-Client Privilege

To the extent the Superior Court concluded that Facebook's public statements nullified any expectation of confidentiality over the Investigation, this conclusion is clearly incorrect. The Superior Court's reasoning here began and ended with a single case—*In re Grand Jury Investigation*, 437 Mass. 340 (2002). There, this Court considered whether a school's attorney-led investigation into child abuse was protected where Massachusetts law required school officials to disclose the results of the investigation to the Department of Children and Families. *Id.* at 350-354. This Court held that privilege never attached to the school's investigation because "[a] quintessential element of the attorney-client privilege—the expectation of confidentiality … [was] absent," because school

officials, as mandatory reporters, knew they would have no right to keep investigation findings secret. *Id.* at 352.

That holding is simply inapposite here. Unlike in *In re Grand Jury Investigation*, here the uncontested record demonstrates that the expectation of confidentiality was and remains a hallmark of the Investigation.[8] A2/51 (¶ 10). Indeed, the Order itself acknowledges this fact, recognizing that at least some communications within the Investigation are privileged. A2/195. That Facebook has publicly noted the general purpose and status of the Investigation does not alter this result.[9] The attorney-client privilege "does not impede disclosure of information except to the extent that that disclosure would reveal confidential communications." *In re Gen. Motors LLC Ignition Switch Litig*., 80 F. Supp. 3d 521, 528-529 (S.D.N.Y. 2015) (quoting *In re Grand Jury Subpoena Duces Tecum (Marc Rich)*, 731 F.2d 1032, 1037 (2d Cir. 1984)).[10] "'[T]he fact that

[8] Integral to this Court's holding in *In re Grand Jury Investigation* was the "duty to preserve the Legislature's prerogative to mandate the disclosure of information." *Id.* at 355.

[9] The Order further defies the undisputed factual record by stating that Facebook "pledged to share information of suspected data misuse uncovered in the course of the ADI with its user community." A2/194. In reality, Facebook committed to notifying individual users of any *actual* misuse of *their own* data that Facebook uncovers. A1/332-333.

[10] The formulation of the attorney-client privilege is identical under Massachusetts and federal law, *compare Comcast*, 453 Mass. at 303, *with Cavallaro v. United States*, 284 F.3d 236, 245 (1st Cir. 2002), and this Court has endorsed federal law governing attorney-client privilege over corporate investigations, *see, e.g.*, *In re*

certain *information* in [otherwise protected] documents might ultimately be disclosed' … does not, by itself, 'create the factual inference that the *communications* were not intended to be confidential at the time they were made.'" *Id.* (emphasis in original) (quoting *Marc Rich*, 731 F.2d at 1037); *see Koch v. Specialized Care Servs., Inc.*, 437 F. Supp. 2d 362, 369 (D. Md. 2005) ("[T]he simple fact that attorney-client communications eventually result in a 'public' communication does not rob the preliminary or prior attorney-client communications of their privileged status.").[11]

2. Facebook Has Not Waived Privilege Over the Investigation

The Order further errs to the extent that it concludes that Facebook implicitly waived its privilege over certain attorney-client communications by "tout[ing]" the Investigation "to the public in an effort to explain or defend its actions."[12] A2/195. Finding implied waiver based on extrajudicial statements that

---

Grand Jury Investigation, 437 Mass. at 351 (citing *Upjohn Co. v. United States*, 449 U.S. 383, 390-392 (1981)), and implied privilege waiver, *see, e.g.*, *Darius v. City of Boston*, 433 Mass. 274, 277-284 (2001) (citing cases).

[11] *See also In re Grand Jury Subpoena*, 341 F.3d 331, 336 (4th Cir. 2003); *In re Feldberg*, 862 F.2d 622, 629 (7th Cir. 1988).

[12] Given that the public statements at issue do not disclose the materials and information called for (*see supra* 19-20; *infra* 34-35), there can be no dispute that the Superior Court did not find that Facebook expressly waived its attorney-client privilege, and the Attorney General does not suggest otherwise. Attorney General's Response to Facebook's Application for Direct Appellate Review, Dkt. 6, at 11-12 (SJC No. DAR-27419).

Facebook has not invoked against the Attorney General in this litigation and that nowhere implicate confidential attorney-client communications would be contrary to this Court's precedent and radically expand the applicability of waiver under Massachusetts law—which might explain why not even the Attorney General argued below that Facebook waived the privilege.[13]

As a threshold matter, the two public statements at issue do not "tout" anything, let alone use the Investigation or its findings to "explain and defend" Facebook's actions. A2/194-195. The first statement merely notes that, as part of the Company'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.

A1/332-333. And the second statement simply provided a general update about the Investigation's progress and restated Facebook's commitment to preventing data misuse:

[13] Because this Court in *In re Grand Jury* found that privilege never existed over the school's investigation in the first instance, it expressly declined to consider whether the defendant waived attorney-client privilege by "tout[ing] its internal investigation to the public in an effort to explain and defend its actions," *id.* at 354, 354 n.24, making the discussion of waiver in *In re Grand Jury* dicta in any event.

> 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.
>
> It is important to understand that the apps that have been suspended are associated with about 400 developers. …
>
> App developers remain a vital part of the Facebook ecosystem. They help to make our world more social and more engaging. But people need to know we're protecting their privacy. And across the board, we're making progress. We won't catch everything and some of what we do catch will be with help from others outside Facebook. Our goal 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 social experiences on Facebook while knowing their data will remain safe.

A2/71-72.

But even if these extrajudicial public statements did "tout" the Investigation to the public (they do not), under Massachusetts law, there can be no implied waiver where Facebook has not affirmatively placed attorney-client communications at issue *in this litigation*. This Court has recognized implicit waiver of privileged communications *only* where a party has used the attorney-client privilege as both a sword and a shield to gain litigation advantage by "injecting certain claims or defenses into a case." *McCarthy v. Slade Assocs., Inc.*, 463 Mass. 181, 191 (2012) (citation omitted). Thus, the touchstone for finding implied waiver is whether the privilege-holder's theory of the case has directly placed protected communications at issue, such as when a party uses portions of an

attorney-client communication as evidence or pleads reliance on an attorney's advice as an element of a claim or defense. *See Clair v. Clair*, 464 Mass. 205, 220 (2013) (finding waiver where privileged communications "are at the heart of proving or disproving the [privilege holder's] counterclaim"); *Global Inv'rs Agent Corp. v. National Fire Ins. Co. of Hartford*, 76 Mass. App. Ct. 812, 818-819 (2010) (finding waiver where plaintiffs "relied on the privileged communications or information to support their allegations").

Nothing of the sort has occurred here. The Attorney General, not Facebook, injected the two public statements at issue into this litigation. A1/34-35; A2/67-73. Facebook has never affirmatively used these statements about the Investigation as a "sword" to advance its case, and there is no basis to justify "pry[ing] open the attorney-client relationship and strik[ing] at the very core of the privilege." *Buster v. George W. Moore, Inc.*, 438 Mass. 635, 654 (2003) (quotation omitted); *In re Keeper of Records (Grand Jury Subpoena Addressed to XYZ Corp.)*, 348 F.3d 16, 25 (1st Cir. 2003) ("Where a party has not thrust a partial disclosure into ongoing litigation, fairness concerns neither require nor permit massive breaching of the attorney-client privilege."); *In re Kellogg Brown & Root, Inc.*, 796 F.3d 137, 146-147 (D.C. Cir. 2015) (reference to internal investigation in court filing did not implicitly 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").[14]

Further, Facebook's public statements cannot give rise to waiver because neither statement discloses or otherwise puts at issue attorney-client communications. *See Darius v. City of Boston*, 433 Mass. 274, 283 (2001) (recognizing forfeiture of privilege only where litigant expressly waives privilege by disclosing attorney-client communications or implicitly waives privilege by putting attorney-client communications at issue in a case); *In re Fluor Intercontinental, Inc.*, 2020 WL 1487700, at *3-4 (4th Cir. Mar. 25, 2020) ("[T]he fact that [defendant's] disclosure covered the same topic as the internal investigation or that it was made pursuant to the advice of counsel doesn't mean that privileged communications themselves were disclosed."); *Cicel (Beijing) Sci. & Tech. Co. v. Misonix, Inc.*, 331 F.R.D. 218, 237 (E.D.N.Y. 2019) ("Plaintiff does not contend that Defendant has put any particular 'privileged communication at issue by relying on it to support a claim or defense'" but rather "asserts only that

[14] *See also In re Lott*, 424 F.3d 446, 455 (6th Cir. 2005) ("It is important to cabin the implied waiver of privileges to instances where the holder of the privilege has taken some affirmative step to place the content of the confidential communication into the litigation."); *Clean Harbors Environmental Servs., Inc. v. Sheppard*, No. SUCV20172013BLS2, 2018 WL 7437046, at *1 (Mass. Super. Dec. 20, 2018) (referencing internal investigation in complaint did not put investigation "at issue" to effectuate implied waiver).

Defendant put the investigation itself, and not any given privileged material, at issue in this case" (citation omitted)).

It is difficult to overstate the practical effects of finding waiver of otherwise privileged communications solely because they "pertain to the results" of a publicly disclosed investigation. A2/195. If allowed to stand, the Order "would ring alarm bells in corporate general counsel offices throughout the country about what kinds of descriptions of investigatory … practices could be used by an adversary to defeat all claims of privilege and protection of an internal investigation." *In re Kellogg Brown & Root*, 796 F.3d at 151. That is, if announcing or generally describing an internal investigation were all it takes to defeat privilege over attorney-client confidences, every company operating in Massachusetts would be incentivized *not* to investigate potential wrongdoing, or to withhold information from the public if it chose to do so. Any disclosure would invite an adversary to seek to use the results of that investigation—and all related confidential communications—against it in unrelated litigation. This is not the law in the Commonwealth.

B. Attorney-Client Privilege Protects Even Purely Factual Communications Made for Purposes of Furthering Legal Advice

In addition to wrongly concluding that Facebook's public statements nullified its privilege over communications pertaining to the results of the Investigation, the Superior Court also erred by finding that certain communications

sought by the CID are not privileged because they are "factual in nature," because they contain "information learned by Facebook during the [Investigation]." A2/194-195. The Order overlooks well-established law that privilege protects disclosure of facts where, as here, such disclosure would necessarily reveal confidential attorney-client communications.

This Court has long recognized that the attorney-client privilege covers communications in which a client provides its lawyer with the facts necessary to render legal advice. *See RFF Family P'ship*, 465 Mass. at 708 ("[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)).

Accordingly, even "purely factual" exchanges are protected from disclosure so long as those facts are gathered at the behest of an attorney for the purpose of providing legal advice and the communications are kept confidential. *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); *see Federal Trade Comm'n v. Boehringer Ingelheim Pharms., Inc.*, 180 F. Supp. 3d 1, 30, 34 (D.D.C. 2016) (attorney-client privilege protects "factual material compiled during a corporation's internal investigation … at counsel's request for later use in providing legal advice" and "extend[s] to communications between corporate employees who are working together to compile facts for in-house counsel to use in rendering legal advice to the company").[15] This fully squares with the "purpose of the privilege"—that is, "to enable clients to make full disclosure to legal counsel of all relevant facts so that counsel may render fully informed legal advice, with the goal of promoting broader public interests in the observance of law and administration of justice." *Commissioner of Revenue v. Comcast Corp.*, 453 Mass. 293, 303 (2009).

Here, as the Superior Court acknowledged, Facebook launched the Investigation specifically "to gather the facts needed to provide legal advice to

[15] *See also General Elec. Co. v. United States*, 2015 WL 5443479, at *1 (D. Conn. Sept. 15, 2015) ("[I]nformation communicated to an attorney in connection with obtaining or rendering legal advice is properly subject to a claim of privilege, even if the information standing alone would not otherwise be subject to a claim of privilege."); *Banks v. Office of Senate Sergeant-At-Arms*, 228 F.R.D. 24, 27 (D.D.C. 2005) (finding that documents that did not expressly contain requests for legal advice were privileged because they recounted facts for use by counsel in providing legal advice).

Facebook about litigation … and other legal risks." A2/183; *see also, e.g.*, A2/48-49 (¶¶ 4-5); A2/54-55 (¶¶ 22-24). The internal communications conveying facts necessary for counsel to weigh the legal risks surrounding the apps reviewed by the Investigation are therefore protected under the attorney-client privilege. Denying privilege to such communications would "limit the valuable efforts of corporate counsel to ensure their client's compliance with the law" by undermining their ability "to gather facts … after being informed of potential misconduct." *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 757, 760 (D.C. Cir. 2014) (quotation omitted).

II. THE WORK PRODUCT DOCTRINE SHIELDS INFORMATION GENERATED IN CONNECTION WITH THE INVESTIGATION

Like the attorney-client privilege, the work product doctrine is a critical part of our adversary system. The Supreme Court has made clear that "it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel." *Hickman v. Taylor*, 329 U.S. 495, 510 (1947). The work product doctrine embodies that principle and "establish[es] … a zone of privacy for strategic litigation planning … to prevent one party from piggybacking on the adversary's preparation." *Comcast*, 453 Mass. at 312 (internal quotation marks omitted); *see also Hickman*, 329 U.S. at 516 (Jackson, J., concurring) ("Discovery was hardly intended to enable a learned profession to perform its functions either without wits or on wits borrowed from

the adversary."); *In re Grand Jury Subpoena*, 274 F.3d 563, 574 (1st Cir. 2001) ("The [work product] rule facilitates zealous advocacy in the context of an adversarial system of justice by ensuring that the sweat of an attorney's brow is not appropriated by the opposing party.").

The Superior Court's Order turns these essential protections on their head. Instead of developing her own investigative criteria and requesting that Facebook produce documents responsive to those criteria, the Attorney General seeks merely to appropriate the work of Facebook's counsel for her own investigative ends. Specifically, the Attorney General demanded that Facebook produce information generated by investigative methodologies that Facebook's counsel developed to assess legal risk to Facebook—exactly contrary to *Hickman*'s and *Comcast*'s teachings. In effect, the Attorney General's request is no different than a party in a civil litigation seeking to compel its adversary to produce an index of the documents the adversary used to investigate the key legal considerations at issue in the case, as well as all communications about those documents. Such a request would be rejected out of hand.

Yet, the Superior Court reached the opposite result—and did so by committing three fundamental errors concerning the scope and application of the work product doctrine. *First*, despite correctly finding that the Investigation was conducted "to provide legal advice to Facebook about litigation" (A2/183), the

Order baselessly concludes that the Investigation is "business as usual" (A2/191), simply because Facebook maintains other routine monitoring, compliance, and enforcement mechanisms unrelated to the Investigation. *Second*, the Superior Court mistakenly concluded that the Investigation was not initiated in anticipation of litigation because it also might promote good business practices. *Finally*, the Superior Court mistakenly held, in the alternative, that if the work product doctrine applies, the Attorney General nonetheless satisfied the standard for piercing work product protections. Those conclusions not only conflict with the weight of authority, a largely undisputed record, and the Superior Court's own findings, they also threaten radically to diminish companies' ability to seek confidential legal advice in moments of crisis and undermine "the vitality of [our] adversary system of litigation." *Comcast*, 453 Mass. at 311.

A. The Investigation Is Not "Business as Usual" for Facebook

The Superior Court concluded that the work product doctrine does not protect materials generated in connection with the Investigation because Facebook employs other routine monitoring, compliance, and enforcement mechanisms *not* conducted in anticipation of litigation. These routine enforcement mechanisms, the Superior Court reasoned, rendered the Investigation "business as usual" for Facebook. A2/191. That conclusion contradicts the law and the facts.

As to the law, this Court has observed that work product protections do not apply to materials that would have been prepared "irrespective of the prospect of litigation." *Comcast*, 453 Mass. at 318 (internal quotation marks omitted); *see also, e.g.*, *United States v. Adlman*, 134 F.3d 1194, 1202 (2d Cir. 1998) ("[T]he 'because of' formulation that we adopt here withholds protection from documents that are prepared in the ordinary course of business or that would have been created in essentially similar form irrespective of the litigation.").[16] But this narrow exception applies only to documents that demonstrably—not hypothetically—would have existed regardless of litigation. As explained by the Second Circuit, whose decision in *Adlman* formed the basis for this Court's holding in *Comcast*, when determining whether a document would have been created irrespective of litigation, courts should not "construct … hypothetical scenario[s]" that "ignore reality." *Schaeffler v. United States*, 806 F.3d 34, 44 (2d Cir. 2015). In *Schaeffler*, counsel was asked to opine on the tax consequences of a transaction. *See id.* The district court concluded that the analysis would have been generated irrespective of litigation by crafting a hypothetical involving "the same

[16] Because Mass. R. Civ. P. 26(b)(3) is "in substantially the same form as the earlier Federal Rules of Civil Procedure, the adjudged construction theretofore given to the Federal rules is to be given to our rules, absent compelling reasons to the contrary or significant differences in content." *Comcast*, 453 Mass. at 316 n.25.

size of the transaction and the same complexity and ambiguity of the tax issues but also a lack of any anticipation of litigation." *Id.* The Second Circuit rejected that unrealistic analysis, concluding that it "posit[ed] a factual situation at odds with reality." *Id.* Such a broad view of the irrespective-of-litigation exception, the Second Circuit concluded, would "virtually swallow the work-product protection." *Id.* at 43.

Courts in the Commonwealth have likewise not given the irrespective-of-litigation exception the expansive scope the Superior Court erroneously allowed. Rather, they have concluded that work product protections shield not only information generated by specialized, lawyer-driven investigations that exceed the scope of other routine policies, but also information generated by routine mechanisms when that information is prepared "because of" litigation. *See Rhodes v. AIG Domestic Claims, Inc.*, No. CIV.A. 05-1360-BLS2, 2006 WL 307911, at *4-5 (Mass. Super. 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."); *Harris v. Steinberg*, No. CIV.A.95-1373G, 1997 WL 89164, at *3-4 (Mass. Super. 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").

The Superior Court's Order ignores this authority and nullifies the work product doctrine's protections by hypothesizing that the documents at issue would have been generated by Facebook even without the threat of litigation—which is both pure speculation and at odds with the undisputed record. The record demonstrates that the Investigation was born amid and because of an actual and anticipated flood of litigations following the Cambridge Analytica incident. *See supra* 15-20. Thus, unlike Facebook's ordinary monitoring, compliance, and enforcement mechanisms, the Investigation involves a retrospective evaluation of potential violations of Facebook's policies and associated legal exposure in connection with an early version of the Facebook Platform. A2/50 (¶ 7). Unlike Facebook's routine programs, the Investigation was designed, and has been overseen since its inception, by outside and in-house counsel, who built the Investigation's framework from the ground up. A2/50-51 (¶ 8). The Investigation's processes and methodologies differ from those Facebook

previously has used to assess compliance with its policies. A2/50-51 (¶ 8). Indeed, before the Investigation commenced, the information the Attorney General seeks did not exist as raw data that counsel could provide to the Attorney General; rather, that information was gathered at the direction of counsel for the purpose of facilitating counsel's provision of legal advice. A2/56-57 (¶ 29). And, were that not enough, the record demonstrates that an investigation of this nature and scope, involving a review of potentially millions of apps to inform Facebook's legal strategy, is not how Facebook typically responds to potential violations of its policies. A2/49 (¶ 5).

These undisputed facts unequivocally demonstrate that the prospect of litigation is the driving force of the Investigation. To construct a hypothetical world in which Facebook faced the same circumstances—extensive media coverage concerning a highly sensitive issue and existing mechanisms designed to detect contemporaneous policy violations rather than investigate potential past violations—but did not anticipate litigation "posits a factual situation at odds with reality." *Schaeffler*, 806 F.3d at 44.[17] Applied in this manner, the irrespective-of-

[17] The Superior Court engaged in precisely this type of speculation. *See, e.g.*, A2/123-124 (50:24-51:5) ("I find it very difficult to believe that in the aftermath of Cambridge Analytica … that Facebook would not have taken -- undertaken some enhanced enforcement program but for the threat of litigation.").

litigation exception would render the protections of the work product doctrine illusory. This is not the law.

B. Whether the Prospect Of Litigation Was Facebook's Primary Motive Is Irrelevant

The Superior Court's order further erred by erecting an additional hurdle to Facebook's work product assertion—namely, that the information generated in the Investigation could not have been prepared "in anticipation of litigation" because the prospect of litigation was not Facebook's primary motive for commencing the Investigation. *See* A2/189; A2/192. Like the remainder of the Superior Court's analysis, this conclusion is at odds with the law.

In *Comcast*, this Court expressly rejected the "primary motive" standard on which the Attorney General's argument is based. 453 Mass at 317 n.28 ("[T]he 'primarily to assist in litigation' test … we have rejected."). Instead, as that decision makes clear, 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." *Id.* at 317.[18] And to determine whether a document was prepared

[18] This Court is by no means alone in seeing the wisdom of such a rule. *See, e.g.*, *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 influenced by the prospects of the litigation."); *In re Grand Jury Subpoena (Mark Torf/Torf Envtl. Mgmt.)*, 357 F.3d

"because of" litigation, courts consider first and foremost whether litigation was pending or reasonably anticipated when the document was created. *See, e.g.*, *id.* at 318 (work product protections shield memorandum drafted because of "reasonable possibility" of litigation); *America's Test Kitchen, Inc. v. Kimball*, No. 1684CV03325BLS2, 2018 WL 2049490, at *5 (Mass. Super. Apr. 2, 2018) (work product protections apply where documents were created after plaintiff "threatened legal action"); *Ace Am. Ins. Co. v. Riley Bros., Inc.*, No. CIV.A. 10-1252-C, 2012 WL 3124620, at *5 (Mass. Super. July 28, 2012) (same where memorandum drafted after insurance company was served with summons).

Had the Superior Court properly applied this Court's holding in *Comcast* to its own finding that Facebook launched the investigation "to provide legal advice to Facebook about litigation," A2/183, it would have been compelled to conclude that the Investigation was undertaken "because of" litigation. Indeed, the undisputed record demonstrates that the prospect of litigation became apparent immediately after the first reports concerning the Cambridge Analytica incident became public in March 2018. A2/48-49 (¶ 4-5). Expectation quickly became reality, as numerous lawsuits and regulatory investigations commenced—including the investigation underlying this dispute. A2/48 (¶ 3); A2/62-66. Faced with these

900, 909-910 (9th Cir. 2004) (documents with "dual purpose character[] fall within the ambit of the work product doctrine").

many pending matters, and the near-certain prospect of many more to come, Facebook's in-house and outside counsel commenced the Investigation. A2/48-51 (¶¶ 3-11). From its inception, the Investigation has been an attorney-driven effort; attorneys have defined its scope, parameters, and operations. A2/48-51 (¶¶ 11). And the Investigation's core purpose is to advise Facebook of its legal positions and risks. *Id.*

That the Investigation also might incidentally promote good business practices, such as assuring users that Facebook takes their privacy seriously, does not change the analysis. In *Comcast*, this Court adopted the "because of" framework precisely because that standard—and not the "primary motive" analysis—ensures that work product protections apply to information that serves multiple purposes. *See* 453 Mass. at 316. This Court rightly concluded that the "because of" standard is "consistent with both the literal terms [of the applicable rule of procedure] and the purposes of the work product doctrine, both of 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." *Id.* (internal quotation marks and citation omitted); *see also id.* at 318 ("[A] litigation analysis prepared so that a party can make an informed business decision is afforded the protections of the work product doctrine."); *America's Test Kitchen, Inc.*, 2018 WL 2049490, at *7 ("So long as the documents

were created because of the threat of litigation, which they were, they fall within the scope of the work product doctrine."). Thus, whether the prospect of litigation was Facebook's primary motive, or whether the Investigation also helped Facebook demonstrate that it was committed to protecting user privacy, is irrelevant. What matters is whether the Investigation was commenced "because of" litigation. And the record leaves no room for doubt that it was.

C. The Information At Issue Constitutes Highly Protected "Opinion" Work Product

Notwithstanding that the very wording of the Attorney General's CID demonstrates her intent to commandeer the legal analysis undertaken by Facebook's counsel, the Superior Court erroneously concluded that she had satisfied the standard for overcoming work product doctrine protections. That alternative holding disregards both the weight of authority and the undisputed record.

The Superior Court's conclusion that the Attorney General seeks "indisputably factual information," *i.e.*, "'fact' work product," A2/192-193, is based on a false dichotomy—with pure fact on one side and pure opinion on the other—that improperly ignores the context in which information is generated. As numerous courts have recognized, even ostensibly "factual" data can reflect counsel's opinions or legal theories. *See, e.g.*, *Salvas v. Wal-Mart Stores, Inc.*, No. 0103645, 2004 WL 616293, at *1 (Mass. Super. Mar. 11, 2004) ("the selection of a

limited number of documents from [a] much greater universe of documents constitutes work product" because it "reflect[s] the thinking and strategy of counsel"); *Smith-Brown v. Ulta Beauty, Inc.*, No. 18 C 610, 2019 WL 2644243, at *5 (N.D. Ill. June 27, 2019) (denying, as "impermissible invasion of work product," request that defendants identify "the people their lawyers selected to interview, *i.e.*, to reveal their lawyers' mental processes"); *United States v. All Assets Held at Bank Julius Baer & Co., Ltd.*, 270 F. Supp. 3d 220, 225 (D.D.C. 2017) (request requiring party "to narrow a list of several hundred individuals … by identifying … those individuals that [defendant's] counsel determined were worth interviewing" would reveal counsel's "legal theories and strategic decisions").

The information the Attorney General's CID seeks exists only as the result of analyses involving attorney-derived criteria and judgment about legal risk. That information reflects the thought processes of counsel concerning, *inter alia*, the types of app features or activities counsel identified as indicating potential policy violations, and where counsel thought Facebook's data and privacy vulnerabilities might potentially lie. In other words, but for the involvement, analysis, and advice of counsel, the lists and other information the Attorney General seeks would not exist. This is quintessential "opinion" work product. The Attorney General's requests are framed in a manner that expressly calls out the legal analysis of

Facebook's counsel concerning the legal risk that certain groups of apps may or may not pose. *See supra* 21-26. Instead of developing her own criteria to investigate potential misuse of Massachusetts residents' Facebook user data, the Attorney General seeks impermissibly to piggyback on the work that Facebook's counsel has undertaken.

Had the Superior Court reached the correct conclusion with respect to that issue, there would have been no need to go any further, since the Attorney General did not come close to making the "highly persuasive showing that the circumstances … are so unusual that protection for opinion work product should be denied." *Comcast*, 453 Mass. at 315. Even accepting the Superior Court's flawed determination that the information at issue is fact work product, however, the Attorney General still has failed to demonstrate a "substantial need" for that information, or that she cannot without "undue hardship" obtain "the substantial equivalent … by other means." *See* Mass. R. Civ. P. 26(b)(3). Facebook has worked cooperatively with the Attorney General since she began her investigation, providing multiple detailed oral and written submissions regarding the Investigation's methods and processes. *See supra* 23-24.

The Attorney General can always develop her own criteria and request additional information based on those criteria. But that is not what she has done here. Rather, the Attorney General appears willing to pursue the information in

question only by co-opting the investigative methodologies and legal analysis of Facebook's counsel. The Attorney General's failure to pursue by commonly accepted and permissible means the information she seeks undermines any claim that she has substantial need for that information and cannot obtain its substantial equivalent by other means.[19]

In sum, the Attorney General has sought improperly to invade Facebook's "zone of privacy for strategic litigation planning," and to "piggyback[]" on counsel's "preparation." *Comcast*, 453 Mass. at 312. That the Attorney General has the authority to investigate the matters at issue does not enable her to pierce work product protections in a way no ordinary civil litigant could ever hope to do. And just as this Court would not compel a defendant in a run-of-the-mill civil action to produce a list of individuals that counsel selected for interviews, or a list of documents responsive to searches designed by counsel to investigate the other party's allegations, so too should it decline to compel Facebook to produce the information at issue here.

---

[19] *Cf. Dyson v. Janson*, No. 0303462, 2004 WL 3091644, at *2 (Mass. Super. Dec. 8, 2004) (no undue hardship where party had opportunity to depose witness concerning same information it sought); *Dedham-Westwood Water Dist. v. National Union Fire Ins. Co. of Pittsburgh*, No. CIV.A. 96-00044, 2000 WL 33419021, at *5 (Mass. Super. Feb. 4, 2000) ("[S]ince [the moving party] has not exhausted all other means of obtaining substantially equivalent materials, its motion is premature and, therefore, must fail.").

III. THERE IS NO WAIVER UNDER MASS. GEN. LAWS CHAPTER 93A, § 6(7)

The Attorney General, in her initial papers before the Superior Court, suggested that Facebook waived its objections to the third CID by choosing to produce materials responsive to non-objected-to portions of the CID and engage in a dialogue about Facebook's objections, rather than refusing all production and immediately commencing litigation under G.L. c. 93A, § 6(7). At oral argument, however, the Attorney General relinquished this argument. A2/156 (83:22-25) (Superior Court: "[Y]ou did make a waiver argument in your papers, are you pressing that?" Assistant Attorney General: "I'm not pressing it[.]"). The Superior Court, in turn, declined to find any waiver under c. 93A, § 6(7), citing this Court's warning against "'passive' non-compliance with a CID," and noting that "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." A2/188 n.3 (quoting *Attorney General v. Bodimetric Profiles*, 404 Mass. 152, 154 (1989)).[20]

[20] The Appeals Court single justice (Kinder, J.) also briefly mentioned a potential waiver under c. 93A, §6(7) when considering Facebook's motion to stay under Mass. R. App. P. 6. That issue was not briefed to the single justice by either Facebook or the Attorney General, and thus the single justice was unaware of the Attorney General's abandonment of the argument. The Attorney General (in opposing Direct Appellate Review) did not suggest waiver was an issue of law presented by this appeal, and the single justice's decision is in any event without precedential effect. *Care & Prot. of M.C.*, 479 Mass. 246, 263-264 (2018); *Matter of Bryan*, 411 Mass. 288, 292 (1991).

The Attorney General was right to abandon this argument. No authority or logic allows a finding of waiver under c. 93A, § 6(7) here, where the record clearly indicates that the Attorney General and Facebook have extensively engaged regarding Facebook's objections from the very outset—and where the Attorney General explicitly declined to ask Facebook to waive any privilege or protection. A1/463 n.1. To find that Facebook in fact did waive its objections while engaging in this dialogue by not *also* commencing expensive and lengthy litigation would be perverse indeed. If that were the law, all CID recipients would be compelled to immediately sue the Attorney General upon receipt of every CID for fear of losing all their objections, thereby hamstringing the Attorney General's investigative processes. That is not the law.

CONCLUSION

The Superior Court's decision should be reversed and the Attorney General's Petition to Compel Compliance With Civil Investigative Demand Pursuant to G.L. c. 93A, § 7, should be denied.

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
Rachel.Gargiulo@wilmerhale.com
Eric.Hawkins@wilmerhale.com
Ivan.Panchenko@wilmerhale.com

ANJAN SAHNI
(admitted *pro hac vice*)
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 vice*)
AMANDA M. AYCOCK
(admitted *pro hac vice*)
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.

July 27, 2020

ADDENDUM

TABLE OF CONTENTS

Page(s)

NOTIFY

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

Attorney General v. Facebook, Inc.

Suffolk Superior Court Action No. 1984CV02597-BLS1

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

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

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

Factual Background

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

Facebook and the Facebook Platform

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

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

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

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

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

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

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

Facebook's Platform Policies and Enforcement Program

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

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

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

Professor Kogan and Cambridge Analytica

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

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

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

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

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

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

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

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

Petition, Exhibit FF.

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

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

Id.

Facebook's App Developer Investigation

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

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

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

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

Id.

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

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

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

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

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

The Attorney General's Investigation

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

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

Id.

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

The Contested Requests

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

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

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

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

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

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

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

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

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

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

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

Discussion

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

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

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

G.L. c. 93A, § 6(1).

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

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

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

I. Applicability of the Work Product Doctrine.

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

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

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

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

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

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

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

The Attorney General argues here that,

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

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

Attorney General's Memo at 19-20.

The Attorney General also asserts that Facebook's ADI,

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

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

Id. at 21.

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

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

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

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

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

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

---

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

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

II. Applicability of the Attorney-Client Privilege.

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

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

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

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

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

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

Id. at 3.

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

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

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

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

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

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

Order

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

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

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

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

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

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

Brian A. Davis
Associate Justice of the Superior Court

Date: January 16, 2020

MASSACHUSETTS RULE OF APPELLATE PROCEDURE 16(K) CERTIFICATION

I hereby certify that, to the best of my knowledge, this brief complies with the Massachusetts Rules of Appellate Procedure Rules 16(a)(13) (addendum), 16(e) (references to the record), Rule 20, and Rule 21, that pertain to the filing of briefs.

1. Exclusive of the exempted portions of the brief, as provided in Mass. R. App. P. 20(a)(2)(D), the brief contains 10,597 words.

2. The brief has been prepared in proportionally spaced typeface using Microsoft Word, version 1808, build 10730.20205 in 14 point Times New Roman font. The undersigned has relied upon the word count feature of this word processing system in preparing this certificate.

/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

July 27, 2020

CERTIFICATE OF SERVICE

I, Felicia H. Ellsworth, hereby certify, under the penalties of perjury that on July 27, 2020, I caused a true and accurate copy of the foregoing to be filed via the Massachusetts Odyssey File & Serve site and served two copies upon the following counsel by electronic and overnight 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