Supreme Judicial Court for the Commonwealth Full Court: SJC-12946 Filed: 11/16/2020 12:00 AM

SJC-12946

IN THE COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

ATTORNEY GENERAL,
Petitioner-Appellee,

v.

FACEBOOK, INC.,
Respondent-Appellant.

On appeal from a judgment of the Superior Court for Suffolk County

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PETITIONER-APPELLEE

CAITRIONA FITZGERALD, BBO #673324
Counsel of Record
ALAN BUTLER
MEGAN IORIO
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
fitzgerald@epic.org

Counsel for Amicus Curiae *EPIC*

November 14, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21, *amicus curiae* Electronic Privacy Information Center ("EPIC") states that it is a District of Columbia corporation with no parent corporation or publicly held company with a 10 percent or greater ownership interest. EPIC is a non-profit, non-partisan corporation, organized under section 501(c)(3) of the Internal Revenue Code.

PREPARATION OF AMICUS BRIEF DECLARATION

Pursuant to Appellate Rule 17(c)(5), *amicus* declares that:

(a) No party or party's counsel authored this brief in whole or in part;

(b) No party or party's counsel contributed money to fund preparing or submitting the brief;

(c) No person or entity other than the *amicus curiae* contributed money that was intended to fund preparing or submitting a brief; and

(d) Counsel has not represented any party in this case or in proceedings involving similar issues, or any party in a case or legal transaction at issue in the present appeal.

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy issues.[1] EPIC regularly participates as *amicus* in federal and state courts in cases concerning consumer privacy. EPIC also advocates for government oversight and regulation of corporate data practices in an increasingly data-driven society.

EPIC has a long sought to hold Facebook accountable for its harmful data practices. In 2009 and 2010, EPIC filed complaints at the FTC arguing that Facebook's policies regarding third-party developers were misleading and deceptive. EPIC et al. FTC Complaint, *In re Facebook* (Dec. 17, 2009);[2] EPIC Supplemental Complaint, *In re Facebook* (Jan. 14, 2010).[3] After the FTC took enforcement action, EPIC urged the agency to strengthen its proposed Consent Order, EPIC Comments, *In re Facebook*, FTC File No. 0923184 (Dec. 27, 2011),[4] and separately asked the Commission to assess whether certain Facebook features

[1] EPIC Appellate Advocacy Fellow Melodi Dincer and EPIC Law Fellow Sara Geoghegan contributed to this brief.
[2] https://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.
[3] http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.
[4] https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf.

violated the Order. Letter from EPIC to Jon Leibowitz, Chairman, FTC (Dec. 27, 2011).[5]

Since 2012, EPIC has filed several detailed complaints with the FTC alleging violations of the Order. *See, e.g.*, Complaint, *In re Facebook, Inc.* (July 3, 2014);[6] Complaint, *In re WhatsApp, Inc.* (Mar. 6, 2014);[7] Complaint, *In re WhatsApp, Inc.* (Aug. 29, 2016);[8] Complaint, *In re Facebook, Inc. and Facial Recognition* (Apr. 6, 2018).[9] EPIC urged the FTC to investigate the unprecedented disclosure of personal data uncovered in the Cambridge Analytica scandal as well. Letter from EPIC et al. to Maureen Ohlhausen, Acting Chairman, FTC, and Terrell McSweeney, Commissioner, FTC (Mar. 20, 2018).[10] EPIC also brought a Freedom of Information Act lawsuit against the FTC to obtain Facebook's privacy assessments, reports, and related records required under the 2012 Order. Complaint for Injunctive Relief, *EPIC v. FTC*, No. 18-942 (D.D.C. filed Apr. 20, 2018).[11] EPIC moved to intervene and filed an *amicus* brief in the FTC's 2019 settlement with Facebook, arguing that

[5] https://epic.org/privacy/facebook/Facebook-Timeline-FTC-Ltr-FINAL.pdf.
[6] https://epic.org/privacy/internet/ftc/facebook/psycho/Facebook-Study-Complaint.pdf.
[7] https://epic.org/privacy/ftc/whatsapp/WhatsApp-Complaint.pdf.
[8] https://epic.org/privacy/ftc/whatsapp/EPIC-CDD-FTC-WhatsApp-Complaint-2016.pdf.
[9] https://epic.org/privacy/facebook/FTC-Facebook-FR-Complaint-04062018.pdf.
[10] https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf.
[11] https://epic.org/foia/ftc/facebook/EPIC-v-FTC-Complaint.pdf.

the settlement failed to protect users. Motion of EPIC to Intervene, *United States v. Facebook, Inc.*, No. 1:19-cv-02184 (D.D.C. July 25, 2019);[12] Br. of *Amicus Curiae* EPIC, *United States v. Facebook, Inc.*, No. 1:19-cv-02184 (D.D.C. filed Dec. 10, 2019).[13]

[12] https://epic.org/privacy/facebook/EPIC-Motion-to-Intervene-FTC-Facebook-Settlement.pdf.
[13] https://epic.org/privacy/facebook/epic2019-challenge/US-v-Facebook-26-EPIC-Amicus-Brief.pdf.

SUMMARY OF THE ARGUMENT

For well over a decade, Facebook has lured in users with promises of privacy. At the same time, the company has maximized its profits by granting third parties access to its vast troves of user data. Facebook has repeatedly undermined user expectations of privacy by unilaterally changing default privacy settings, modifying its policies for protecting user data, and allowing third parties access to users' data without their knowledge or consent.

Facebook has been on notice of third-party app abuse for nearly as long as the company has allowed third parties access to user data. The company has also been under a legal obligation to adopt business practices that safeguard that data for just as long. Indeed, improper third-party access to user data was at the core of the FTC's 2011 Complaint and 2012 Consent Order against Facebook. Under the 2012 FTC Consent Order, Facebook was required to implement a comprehensive privacy program to monitor for and prevent further abuse. If Facebook had fulfilled its monitoring obligations, it would have caught and potentially prevented the Cambridge Analytica incident and other abuses before a threat of litigation existed. Clearly, Facebook has it backwards: the App Developer Investigation (ADI) is not the result of a litigation threat; the litigation threat is a result of Facebook's failure to proactively monitor for the activities uncovered by the ADI, as it was obligated

to do. This Court should not reward Facebook for ignoring its legal obligations until there was a threat of litigation.

In contrast to Facebook's cavalier attitude towards user privacy over the years, the company has assiduously protected its own privacy through a pattern of secrecy. When it comes to user privacy, ad targeting, and anti-disinformation efforts, Facebook has used a combination of vacuous public relations ploys, misleading statements, obstruction, and litigation to prevent the public from understanding how it handles threats to users and their data. The result is that Facebook knows a shocking amount about each of its users, but its users know shockingly little about Facebook. This information asymmetry threatens the public interest. Without transparency, Facebook will continue to evade accountability and the harmful effects of Facebook's business practices could go undetected.

Given the FTC's failure to impose public transparency requirements on Facebook, investigations like that of the Attorney General are the public's only hope for transparency and accountability. If the Attorney General is unable to obtain the information at issue, the public may never know the extent of Facebook's breach of the public trust.

ARGUMENT

I. Facebook should not be rewarded for ignoring its privacy obligations.

Facebook has profited from its ability to attract users with false promises of privacy. Over a billion users have been lured to the platform under the premise that their data would be protected. For more than a decade, these users have relied on Facebook's representations to their detriment. The company has faced intense scrutiny and has been sued numerous times for ignoring its privacy obligations. Facebook could have avoided scandal and litigation by adopting appropriate business practices that safeguard user data, as it is obligated to do. Instead, Facebook has repeatedly turned a blind eye to known privacy risks. The company's scandals follow a predictable cycle: Facebook attracts users by promising to protect their private data; the company instead makes that data available to third parties without their knowledge or consent; Facebook fails to otherwise adopt adequate safeguards to protect user data; Facebook is on notice that third parties are improperly accessing user data but does not prevent the abuse; Facebook is investigated or sued and obligated to adopt business practices in line with its initial promises of user privacy; Facebook's CEO apologizes for the company's "mistake;" and then Facebook inevitably fails to meet these obligations yet again.

See Zeynep Tufekci, *Why Zuckerberg's 14-Year Apology Tour Hasn't Fixed Facebook*, Wired (Apr. 6, 2018).[14]

Facebook's privacy obligations precede the litigation threats the company faces. The information at issue in this case should have been revealed during Facebook's normal business practice of monitoring third party access to user data, as it is obligated to do under the 2012 Consent Order. The fact that Facebook ignored its privacy obligations should not justify secrecy now. This Court should not reward Facebook for sleeping on its privacy obligations and waiting until there was a litigation threat to look into the known risk of third-party data abuse at issue in this case.

In its infancy, Facebook committed to protecting user privacy to attract users from competing sites like MySpace, which made little effort to protect personal data. Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 Cal. Bus. L.J. 39, 48 (2019).[15] For the first few years, Facebook was a closed network whose privacy policy explicitly promised not to track users or collect their data for commercial purposes, allowed users to prohibit Facebook

[14] https://www.wired.com/story/why-zuckerberg-15-year-apology-tour-hasnt-fixed-facebook/.
[15] https://lawcat.berkeley.edu/record/1128876.

from collecting third-party data about them, and gave users the ability to opt-out of disclosing their information to third parties. *Id.* at 49–51.

In 2007, the company first broke its privacy promise to its then-50 million users with an advertising program called Beacon. The program published users' personal information, including online purchases and browsing habits, from third-party sites by default without first obtaining user consent. David C. Vladeck, *Facebook, Cambridge Analytica, and the Regulator's Dilemma: Clueless or Venal?*, Harv. L. Rev. Blog (Apr. 14, 2018).[16] Facebook initially denied that Beacon tracked users across the web without their consent. *See* Srinivasan, *supra*, at 57. Facebook eventually backtracked after a researcher confirmed the extent of Beacon's tracking and data collection. *Id.* at 58. Facebook was a defendant in multiple federal lawsuits[17] and stopped the program two years later pursuant to a $9.5 million settlement. David Kravets, *Judge Approves $9.5 Million Facebook 'Beacon' Accord*, Wired (Mar. 17, 2010).[18]

The same year Facebook rolled out Beacon, it also made several changes that introduced new risks for users and made it easier for third parties like

---

[16] https://blog.harvardlawreview.org/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/.
[17] *See, e.g.*, Lane v. Facebook, Inc., No. 5:08-CV-03845 (N.D. Cal. filed Aug. 12, 2008); Harris v. Facebook, Inc., No. 09-01912 (N.D. Tex. filed Oct. 9, 2009); *see also* Harris v. Blockbuster, No. 09-217 (N.D. Tex. filed Feb. 3, 2009), *appeal docketed*, No. 09-10420 (5th Cir. Apr. 29, 2009).
[18] https://www.wired.com/2010/03/facebook-beacon-2/.

Cambridge Analytica to improperly obtain user data without the user's knowledge or consent. In one change, Facebook partnered with at least sixty third-party device manufacturers, including Apple, Amazon, BlackBerry, Microsoft, and Samsung, and enabled them to access and store user data without user consent; most of these partnerships remained in place through 2018. Gabriel J.X. Dance et al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018).[19]

The most significant turning point for user privacy came when Facebook unveiled the Platform, which allowed third-party app developers to integrate their apps with Facebook and access user data. Facebook, *Facebook Unveils Platform for Developers of Social Applications* (May 24, 2007).[20] Initially, the default setting only allowed third-party apps that a user registered with to access the user's name and network unless the developer obtained opt-in permission to access more granular types of information. EPIC et al. FTC Complaint, *In re Facebook*, ¶ 36, 57 (Dec. 17, 2009).[21] Facebook did not closely monitor the permissions that developers requested, and a 2007 study of third-party apps on the Platform found that Facebook allowed over 90% of apps to obtain more data-access privileges than

---

[20] https://about.fb.com/news/2007/05/facebook-unveils-platform-for-developers-of-social-applications/.
[21] https://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

needed for the apps to perform. Adrienne Felt & David Evans, Univ. of Va., *Privacy Protection for Social Networking APIs*.[22]

Then, in 2009, Facebook unilaterally changed its privacy settings to make previously private information "publicly available" to third-party app developers and websites by default. Bill Goodwin and Sebastian Klovig Skelton, *Facebook's Privacy Game – How Zuckerberg Backtracked on Promises to Protect Personal Data*, ComputerWeekly.com (July 1, 2019).[23] The changes allowed any third-party app, search engine, and website to access personal data such as a user's name, gender, city, profile photo, friends list, liked pages, and network membership. EPIC FTC Complaint, *supra*, at ¶ 34. Such information could reveal a user's sexual orientation and political beliefs, *id.* at ¶¶ 45, 47, and put political dissidents and their relatives in danger from authoritarian regimes, *id*. at ¶¶ 48-53. Importantly, Facebook also eliminated users' previous ability to opt out of all data disclosures to third parties. *Id.* at ¶ 70. Users did not consent to any of these changes.

Soon after Facebook announced these material policy changes, EPIC and others filed a complaint with the FTC alleging Facebook had engaged in unfair and

---

[22] https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=F5AD563B5C0577BF12CA9BAD50178FAA?doi=10.1.1.143.7761&rep=rep1&type=pdf (last accessed Nov. 12, 2020).

[23] https://www.computerweekly.com/feature/Facebooks-privacy-U-turn-how-Zuckerberg-backtracked-on-promises-to-protect-personal-data#Promise-1.

deceptive business practices when it violated user expectations, diminished user privacy, and contradicted the company's own representations. *See* EPIC FTC Complaint, *supra*. In response, the FTC stated that the complaint "raise[d] issues of particular interest for us at this time," and soon opened an investigation into Facebook's business practices. Letter from Director, FTC Bureau of Consumer Protection, to Marc Rotenberg, Director, EPIC (Jan. 14, 2010).[24]

In 2010, while the FTC investigation was ongoing, Facebook again reneged on its promise to protect user privacy by re-establishing a Beacon-like tracking system across the web. Facebook offered tens of thousands of websites the ability to install a "Like" button that could track users' activities. Srinivasan, *supra*, at 63. When Zuckerberg first announced the Like button, he failed to mention that it could be used to track users as they moved across the internet without their consent. *Id.* at 64. The company later stated that it would not use the Like button to collect data for advertising. *Id.* at 65. Researchers subsequently found that, in reality, Facebook did track users and even non-users through the Like button. *Id.* at 66. Facebook insisted the Like button was "not intended for tracking," the researchers had found a "bug," and that it would discontinue any inadvertent tracking. *Id.* Even after this announcement, other researchers showed that Facebook continued to track users. *Id.* at 66-67. During this time period, Facebook

[24] https://epic.org/privacy/inrefacebook/Facebook_Vladeck_Letter.pdf.

also filed an application for a patent for a "method . . . for tracking information about the activities of users of a social network system while on another domain." *Id.* at 68.

The FTC wrapped up its investigation in 2011 and formally charged Facebook with eight counts of unfair and misleading business practices, including deceptive privacy settings. Complaint, *In re Facebook* (Nov. 29, 2011).[25] Among the FTC's findings were that Facebook deceived users into believing that they could limit the extent of third parties access to data on the Platform when in fact users had no such power to limit the amount of information disclosed to apps by default. *Id.* at ¶¶ 17–28. In a 2012 Consent Order, the FTC barred Facebook from making further deceptive privacy claims, required the company to get user approval before changing their data practices again, and prohibited Facebook from disclosing user data to third parties without giving users clear notice and obtaining their "affirmative express consent." Decision and Order, *In re Facebook* (Aug. 10, 2012);[26] *see also* Vladeck, *supra*. The Order also required extensive changes to Facebook's business practices. Facebook was to establish a monitoring system to proactively detect and deter privacy abuses by third parties, assess risks to

[25] https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf.
[26] https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

consumer privacy and take reasonable measures to counteract them, submit to twenty years of privacy audits, and provide biennial reports on their privacy practices. Decision and Order, *supra.*

Over the next several years, Facebook failed to change its business practices and to fix its broken privacy promises. In particular, Facebook failed to implement a key requirement of the 2012 Consent Order: to maintain a reasonable privacy program to actively monitor and prevent app abuses. Complaint, *United States v. Facebook, Inc*., No. 19-cv-2184, ¶ 10 (D.D.C. filed July 24, 2019).[27] This failure led directly to the Cambridge Analytica scandal.

Just four months after the Order was finalized, Facebook began once again to mislead users about what information third parties could access. The company removed a disclaimer that had warned users that personal data made available to their Facebook friends would also be disclosed to the apps used by their friends. See *Id.* at ¶ 7, 35-36. In 2014, Facebook began to limit third party access to friends' data but made special arrangements with dozens of whitelisted developers to allow them to continue to collect friends' data through June 2018. *Id.* at ¶ 8. In its 2019 settlement with Facebook, the FTC found that Facebook knew or should

[27] https://www.courtlistener.com/recap/gov.uscourts.dcd.209448/gov.uscourts.dcd.209448.1.0_1.pdf.

have known that this conduct violated the 2012 Consent Order because it was "the very same conduct" that led to the Order. *Id.* at ¶ 9.

The FTC determined that Facebook's failure to maintain a reasonable privacy program was influenced by the financial benefits the company obtained from violator apps. *Id.* at ¶ 12. To make matters worse, Facebook did closely monitor third-party data access under certain circumstances: when its profits and control of the market were at stake. Facebook monitored third-party access to user data to restrict competing companies' ability to grow their apps—not to protect users' privacy. Olivia Solon and Cyrus Farivar, *Mark Zuckerberg Leveraged Facebook User Data to Fight Rivals and Help Friends, Leaked Documents Show*, NBC News (Apr. 16, 2019).[28]

Facebook cannot reasonably claim that the results of the ADI should be kept secret because they were solely related to post-Cambridge Analytica litigation. The Cambridge Analytica incident began two years into Facebook's compliance period with the Order, five years after EPIC and others complained to the FTC about Facebook's deceptive privacy practices concerning third-party apps, and seven years after Facebook first faced public backlash after promising to protect user privacy while actively disclosing user data to third parties without consent. The

[28] https://www.nbcnews.com/tech/social-media/mark-zuckerberg-leveraged-facebook-user-data-fight-rivals-help-friends-n994706#anchor-SELLDATAFOR.

litigation threats are a result of Facebook's failure to proactively monitor the activities uncovered in the ADI, as the company was legally required to do. Facebook also should have reported any unauthorized disclosure of user data to the FTC and to the independent auditor charged with assessing the company's privacy practices under the Order. If Facebook had complied with its privacy obligations, the incident may have never occurred. At the very least, the information would be discoverable today. For that reason alone, this Court should reject Facebook's attempt to use litigation threats as an excuse to prevent the facts of its breach of user trust from coming to light.

II. Facebook's pattern of secrecy obscures the company's impact on the public.

Given how careless Facebook has been with the privacy of its users over the years, it is hard to take seriously the company's charge that the Attorney General seeks to "improperly invade Facebook's 'zone of privacy'" with its information request. Br. for Respondent-Appellant at 54. Facebook profits off the personal data of its users. Yet, Facebook consistently refuses to provide users or the public with essential information about its data practices. From privacy to ad targeting to anti-disinformation efforts, Facebook often promises transparency as a public relations ploy but rarely delivers in a meaningful way. Instead, Facebook uses obstruction, litigation, and the threat of litigation to prevent the public from understanding the company's practices. The information asymmetry caused by Facebook's pattern of

secrecy is especially dangerous because of the outsized role Facebook plays in society. Without greater public transparency, individuals cannot make informed decisions about whether and to what extent to use Facebook, governments cannot effectively regulate the company, and society cannot hold it accountable for its transgressions.

One key example is Facebook's intervention in EPIC's FOIA case to prevent the public from viewing the biennial privacy assessments mandated by the 2012 Consent Order. EPIC and other advocates have pressed Facebook and the FTC to make the assessments public since the beginning. Before the 2012 Order was even finalized, EPIC urged the FTC to require Facebook to make the assessments publicly available. EPIC Comments, *In re Facebook*, FTC File No. 0923184, at 2 (Dec. 27, 2011).[29] After the FTC failed to do so, EPIC filed a FOIA request seeking Facebook's first privacy assessment soon after the assessment was due. Letter from EPIC to the Office of General Counsel, FTC (Apr. 26, 2013).[30] The FTC ultimately published heavily redacted versions of the assessments, likely due to Facebook's objections to public release. *See* Complaint for Injunctive Relief, *EPIC v. FTC*, No. 18-942, ¶ 33 (D.D.C. filed Apr. 20, 2018).[31]

[29] https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf.
[30] https://epic.org/privacy/ftc/FOIA-Facebook-Assessments.pdf.
[31] https://epic.org/foia/ftc/facebook/EPIC-v-FTC-Complaint.pdf.

Following the Cambridge Analytica revelations, EPIC once again submitted a FOIA request for the unredacted assessments and related communications between Facebook and the FTC, *id.* at ¶¶ 19, 26, and then sued for their release, *id.* Facebook intervened in the case and attempted to shield the information from public view. Motion by Facebook, Inc. to Intervene, *EPIC v. FTC*, No. 18-942 (D.D.C. filed May 3, 2019).[32] Facebook opposed EPIC's transparency request because it claimed the records would reveal "to the public at large" Facebook's "sensitive business information" such as its "internal policies and practices" for protecting user privacy. *Id*. at 7. As a result, the public still cannot review the full privacy assessments and cannot determine how Facebook and the FTC failed to detect and report on Cambridge Analytica and related incidents. *See* PwC, *Independent Assessor's Report on Facebook's Privacy Program* (2013);[33] PwC, *Independent Assessor's Report on Facebook's Privacy Program* (2015);[34] PwC, *Independent Assessor's Report on Facebook's Privacy Program* (2017).[35]

[32] https://epic.org/foia/ftc/facebook/EPIC-v-FTC-18-942-FB-Motion-to-Intervene-050319.pdf.
[33] https://epic.org/foia/FTC/facebook/EPIC-18-03-20-FTC-FOIA-20180626-FB-Assessment-2013.pdf.
[34] https://epic.org/foia/FTC/facebook/EPIC-18-03-20-FTC-FOIA-20180626-FB-Assessment-2015.pdf.
[35] https://epic.org/foia/FTC/facebook/EPIC-18-03-20-FTC-FOIA-20180626-FB-Assessment-2017.pdf.

Facebook has also used public relations ploys, obfuscation, and litigation to prevent the public from understanding how Facebook targets advertisements to users. For years, researchers have raised alarms about discriminatory and manipulative ad targeting on Facebook. *See, e.g.*, Julia Angwin and Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race*, ProPublica (Oct. 28, 2016);[36] Gillian B. White, *When Algorithms Don't Account for Civil Rights*, Atlantic (Mar. 7, 2017);[37] *Targeted Facebook Ads Shown to Be Highly Effective in the 2016 US Presidential Election*, Science News (Oct. 25, 2018);[38] Scott Shane and Sheera Frenkel, *Russia 2016 Influence Operation Targeted African-Americans on Social Media*, N.Y. Times, (Dec. 17, 2018);[39] Muhammad Ali et al., *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes*, 3 Proceedings of the ACM on Human-Computer Interaction 1 (Nov. 2019).[40] Because Facebook refused to provide the public with data on the ads it showed users and how they were targeted, researchers resorted to scraping the data through various tools, including plug-ins that internet users installed on

[36] https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.
[37] https://www.theatlantic.com/business/archive/2017/03/facebook-ad-discrimination/518718/.
[38] https://www.sciencedaily.com/releases/2018/10/181025103303.htm.
[39] https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html.
[40] https://www.ccs.neu.edu/home/amislove/publications/FacebookDelivery-CSCW.pdf.

their browsers. *See, e.g.,* Jeremy B. Merrill and Ariana Tobin, *Facebook Moves to Block Ad Transparency Tools – Including Ours*, ProPublica (Jan. 28, 2019).[41] Facebook responded by continuously changing the code on its site to prevent the researchers from automatically collecting ad data. *Id.*; Jim Waterson, *Facebook Restricts Campaigners' Ability to Check Ads for Political Transparency*, The Guardian (Jan. 27, 2019).[42]

At the same time Facebook was obstructing independent transparency efforts, the company made a public commitment to combat disinformation ahead of the 2019 European Union elections. European Comm'n, *Roadmaps to Implement the Code of Practice on Disinformation* (Oct. 16, 2018).[43] Researchers and advocates pushed Facebook to make good on its promises to fight disinformation by releasing its ad data, Mozilla, *Open Letter to Facebook* (2019),[44] and Facebook responded by announcing the Ad Library API. A Facebook executive called the move "a new level of transparency for ads on Facebook." Rob

[41] https://www.propublica.org/article/facebook-blocks-ad-transparency-tools#:~:text=Politics-,Facebook%20Moves%20to%20Block%20Ad%20Transparency%20Tools%20%E2%80%94%20Including%20Ours,shut%20it%20down%20last%20year.
[42] https://www.theguardian.com/technology/2019/jan/27/facebook-restricts-campaigners-ability-to-check-ads-for-political-transparency.
[43] https://ec.europa.eu/digital-single-market/en/news/roadmaps-implement-code-practice-disinformation.
[44] https://foundation.mozilla.org/en/campaigns/eu-misinformation-facebook/.

Leathern (@RobLeathern), Twitter (Feb. 11, 2019, 1:02 PM).[45] But the tool that Facebook released proved completely inadequate: it was difficult to search, it was impossible to tell whether it was comprehensive, and it failed to provide the public with any information about the targeting criteria advertisers used. *See* Mozilla, *Facebook's Ad Archive API is Inadequate* (Apr. 29, 2019).[46]

Instead of improving its API, Facebook instead ramped up its campaign against independent transparency efforts. One particularly influential ad data aggregator is the NYU Ad Observatory, which journalists from around the country have relied upon for information on Facebook ad targeting. Mozilla, *Dear Facebook: Withdraw Your Cease & Desist to NYU* (Oct. 28, 2020).[47] Just a few weeks before the 2020 election, Facebook threatened to sue the NYU Ad Observatory unless it discontinued its ad transparency database and deleted all of its data. Jeff Horwitz, *Facebook Seeks Shutdown of NYU Research Project into Political Ad Targeting*, Wall St. J. (Oct. 23, 2020).[48] Facebook unironically claimed that the tool threatened user privacy. Rob Leathern (@RobLeathern), Twitter (Oct. 24, 2020, 8:46 PM).[49] The researchers said they would halt their

---

[45] https://twitter.com/robleathern/status/1095020163127115776.
[46] https://blog.mozilla.org/blog/2019/04/29/facebooks-ad-archive-api-is-inadequate/.
[47] https://foundation.mozilla.org/en/blog/dear-mr-zuckerberg//
[48] https://www.wsj.com/articles/facebook-seeks-shutdown-of-nyu-research-project-into-political-ad-targeting-11603488533.
[49] https://twitter.com/robleathern/status/1320164751696068612.

collection efforts if Facebook released the data themselves. Horowitz, *supra*. Facebook has met this call with silence.

Facebook also failed to fulfill its promise to provide information on its anti-disinformation efforts to the European Commission ahead of the 2019 elections. Facebook made a big public display of announcing a "war room" to fight disinformation, Alex Hern, *Facebook to Create 'War Room' to Fight Fake News, Nick Clegg Says*, Guardian (Jan. 28, 2019), and signed a voluntary code of conduct with the European Commission promising to disclose information about its anti-disinformation efforts. European Comm'n, *supra.* But in the run-up to the elections, Facebook had only set up factcheckers in eight of the EU's 28 member states and otherwise failed to provide "hard numbers" to show that it was following through on its promises. Daniel Boffey, *Facebook Withholding Data on Its Anti-Disinformation Efforts, EU Says*, Guardian (Feb. 27, 2019).[50]

Facebook also responded to calls for added anti-disinformation efforts ahead of the 2020 U.S. elections by announcing it was "committed to . . . providing transparency." Facebook, *Preparing for Elections* (2020).[51] Yet, a key tool for state officials to track election disinformation did not include data on the primary sources of such information: posts from individual users and private Facebook

[50] https://www.theguardian.com/technology/2019/feb/28/facebook-withholding-data-anti-disinformation-efforts-eu.
[51] https://about.fb.com/actions/preparing-for-elections-on-facebook/.

groups. Tech Transparency Project, *Facebook Leans on States to Spot Voter Interference* (Sep. 23, 2020).[52] A Facebook executive even admitted that the information tracked by the tool represented only a "tiny [percentage]" of the posts most people see on the site, significantly mitigating its usefulness. John Hegeman (@johnwhegeman), Twitter (Jul. 20, 2020, 7:38 PM).[53]

This Court has an opportunity to disrupt Facebook's pattern of secrecy. Public transparency is the only path to accountability. The Attorney General's investigation is key to this effort.

III. The Attorney General should have access to the requested information because it is the only way for the public to learn of Facebook's data practices.

Time and again, Facebook has dodged accountability. The FTC has consistently failed to enforce Facebook's legal obligations, and the company has otherwise evaded public accountability. Even after two FTC enforcement actions and a string of major privacy breaches, Facebook's privacy practices remain opaque. State government investigations like the one at issue in this case are essential to protecting the public's interest in understanding Facebook's business practices and ensuring that the company complies with its obligations.

[52] https://www.techtransparencyproject.org/articles/facebook-leans-states-spot-voter-interference.
[53] https://twitter.com/johnwhegeman/status/1285358531214888960.

The FTC made a grave mistake when it failed to aggressively monitor Facebook's privacy practices following the 2012 Consent Order. After EPIC and others forced partial release of Facebook's privacy audits, it was revealed that Facebook and the auditors had missed many significant problems. For example, the 2017 audit report, which should have uncovered the Cambridge Analytica incident, found that Facebook's privacy controls "provide[d] reasonable assurance to protect the privacy of covered information." PwC, *Independent Assessor's Report on Facebook's Privacy Program* (2017);[54] Nicholas Confessore, *Audit Approved of Facebook's Policies, Even After Cambridge Analytica Leak*, N.Y. Times (Apr. 19, 2018).[55] Obviously, they did not.

The lack of transparency about what Facebook was doing enabled prolonged inaction by the FTC, which had taken responsibility for policing Facebook's privacy practices when it entered into the Consent Order. When Facebook repeatedly failed to assure the FTC that it was meeting its obligations, the Commission expressed disappointment with Facebook's secrecy and concern over Facebook's suspect practices but refused to declare that Facebook was in violation of the Order. *See, e.g.*, Email from Reenah L. Kim, Counsel, FTC, to Ashlie S.

---

[54] https://www.ftc.gov/system/files/documents/foia_requests/02.12.15_-_02.11.17_fb_privacy_assessment.pdf.

[55] https://www.nytimes.com/2018/04/19/technology/facebook-audit-cambridge-analytica.html.

Beringer et al., Counsel, Gibson, Dunn & Crutcher, LLP (Sept. 11, 2013, 11:35 EST).[56] The Commission was reluctant to enforce the Order, hedging its criticism by saying that a noncompliant data practice "appear[ed] to implicate" an obligation or "likely create[d] deception." Letter from Reenah L. Kim & Laura D. Koss, Counsel, FTC, to Ashlie Beringer, Counsel, Gibson, Dunn & Crutcher, LLP (Sept. 30, 2013);[57] Letter from Reenah L. Kim, Counsel, FTC, to Edward Palmieri & Robert Sherman, Counsel, Facebook (Apr. 12, 2016).[58]

The FTC eventually took legal action against Facebook for violating the 2012 Order, but the resulting settlement largely imposed the same obligations the company had previously flouted. Even the judge who entered the final order admitted that, while the settlement passed muster under the deferential standard applied, "the Court might well have fashioned different remedies were it doing so out of whole cloth after a trial." *Id.* at 124. The judge went on to describe Facebook's conduct as "stunning," "unscrupulous," "shocking," and "underhanded." *United States v. Facebook, Inc.*, 456 F. Supp. 3d 115, 117, 122, 121 (D.D.C. Apr. 23, 2020).

---

[56] https://epic.org/foia/ftc/facebook/EPIC-18-03-20-FTC-FOIA-20181019-FTC-FB-Addtl-Communications-2013.pdf.
[57] https://epic.org/foia/ftc/facebook/EPIC-18-03-20-FTC-FOIA-20181019-FTC-20130920-Letter.pdf.
[58] https://epic.org/foia/ftc/facebook/EPIC-18-03-20-FTC-FOIA-20181019-FTC-AccountKit-Letter.pdf.

Several FTC Commissioners rejected the 2019 settlement as inadequate precisely because it failed to obtain sufficient public transparency over Facebook's privacy practices. Commissioner Chopra believed the FTC "cut off the inquiry too early, leaving too many stones unturned," and "should have continued the investigation to obtain more data and evidence." Dissenting Statement of Comm'r Rohit Chopra at 19-20, *In re Facebook, Inc.* (July 24, 2019).[59] The settlement instead allowed Facebook to "decide for itself how much information it can harvest from users and what it can do with that information, as long as it creates a paper trail." *Id.* at 1. Commissioner Slaughter criticized the settlement's failure to include "meaningful limitations on data collection and sharing and substantial *public* transparency about Facebook's data use and order compliance." Dissenting Statement of Comm'r Rebecca Kelly Slaughter at 12, *In re Facebook, Inc.* (July 24, 2019) (emphasis in original).[60] Unlike a settlement, litigation "would have provided public transparency and accountability for the company" by forcing Facebook to publicly disclose information about its data practices once and for all. *Id.* at 7.

[59] https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.
[60] https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf.

If Facebook will not proactively disclose information about the third parties that abused user data, and the FTC will not force it to do so, then the Attorney General's investigation is the public's only hope. For the sake of transparency, advocacy, and safeguarding consumer privacy, the Attorney General should have access to this information.

CONCLUSION

Amicus EPIC respectfully requests that this Court affirm the Superior Court's order granting the Attorney General's petition to compel compliance with Civil Investigative Demand No. 2018-CPD-67.

Respectfully submitted,

*/s/ Caitriona Fitzgerald*_____
Caitriona Fitzgerald
Counsel of Record
Alan Butler
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

CERTIFICATE OF COMPLIANCE

I hereby certify that the above brief complies with the rules of court that pertain to the filing of brief, including, but not limited to: Rule 16(a)(13); Rule 16(e); Rule 18; Rule 20; and Rule 21. This brief complies with the type-volume limitation of Rule 20(2)(C) because it contains 4,843 words, excluding the parts of the brief limited by the rule. It complies with the type style requirements of Rule 20 because it has been prepared in proportionally spaced typeface using Microsoft Office Word in 14-point Times New Roman style.

Dated: November 14, 2020 */s/ Caitriona Fitzgerald*_____

Caitriona Fitzgerald
Counsel of Record
Alan Butler
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on November 14, 2020, this brief was electronically filed with the Clerk of the Court for the Supreme Judicial Court and served upon the following counsel of record through the Electronic Filing System:

Sara Cable, A.A.G. (Sara.cable@mass.gov)
Peter N. Downing, A.A.G (Peter.downing@mass.gov)
Jared Rinehimer, A.A.G. (Jared.rinehimer@mass.gov)
Office of the Attorney General
Consumer Protection Division
One Ashburton Place
Boston, MA 02108

I further certify that on November 14, 2020, I served true copies of this brief by email to the following counsel of record who are not registered users:

Felicia H. Ellsworth, Esq. (*felicia.ellsworth@wilmerhale.com*)
Rachel L. Gargiulo, Esq. (*rachel.gargiulo@wilmerhale.com*)
Eric L. Hawkins, Esq. (*eric.hawkins@wilmerhale.com*)
Paloma Naderi, Esq. (*paloma.naderi@wilmerhale.com*)
Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, MA 02109
(617) 526-6000

Dated: November 14, 2020 *<u>/s/ Caitriona Fitzgerald</u>*_____

Caitriona Fitzgerald
Counsel of Record
Alan Butler
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140