XAVIER BECERRA
Attorney General of California
NICKLAS A. AKERS (SBN 211222)
Senior Assistant Attorney General
STACEY D. SCHESSER (SBN 245735)
Supervising Deputy Attorney General
LISA B. KIM (SBN 229369)
MICAH C.E. OSGOOD (SBN 255239)
SUSAN SAYLOR (SBN 154592)
MANEESH SHARMA (SBN 280084)
Deputy Attorneys General
455 Golden Gate Ave. Suite 11000
San Francisco, CA 94102
Telephone: (415) 510-3500
mike.osgood@doj.ca.gov
Attorneys for People of the State of California

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN FRANCISCO

PEOPLE OF THE STATE OF CALIFORNIA EX REL. XAVIER BECERRA, ATTORNEY GENERAL, Petitioner, **v.** **FACEBOOK, INC.,** Respondent.	EXEMPT FROM FILING FEES PER GOV. CODE § 6103 Case No. CPF-19-516916 **PETITION TO ENFORCE INVESTIGATIVE SUBPOENA AND INVESTIGATIVE INTERROGATORIES** (GOV. CODE, §§ 11180 et seq.)

1. In 2018, California Attorney General Xavier Becerra launched an investigation into the business practices of Facebook Inc., following widespread reports that Facebook allowed third parties to harvest Facebook users' private information. What initially began as an inquiry into the Cambridge Analytica scandal expanded over time to become an investigation into whether Facebook has violated California law by, among other things, deceiving users and ignoring its own policies in allowing third parties broad access to user data.

2. Early in the investigation, the Attorney General used his pre-litigation investigatory powers granted by section 11180 *et seq.* of the Government Code to issue an investigative subpoena requiring Facebook to produce documents relating to the Cambridge Analytica matter. A year passed before Facebook completed its drawn-out response to the subpoena, during which time the Attorney General also issued a first set of investigative interrogatories.

3. On June 17, 2019, the Attorney General served a second set of interrogatories and a further subpoena to delve deeper into matters disclosed in Facebook's initial responses and later news reports concerning other claims of wrongdoing by Facebook over users' privacy. Facebook's responses to this second subpoena and set of interrogatories is patently deficient. Despite repeated entreaties, Facebook has provided no answers for nineteen interrogatories and produced no new documents in response to six document requests. Facebook has also wholly refused to search communications involving senior executives for responsive materials. Thus, Facebook is not just continuing to drag its feet in response to the Attorney General's investigation, it is failing to comply with lawfully issued subpoenas and interrogatories.

4. Accordingly, the People of the State of California, acting through Attorney General Xavier Becerra, petition this Court pursuant to section 11188 of the Government Code to enforce compliance with the Attorney General's investigative subpoena and interrogatories. This investigation involves serious allegations of unlawful business practices by one of the richest companies in the world, prompting inquiries by Congress, European and U.S. regulators at the state and federal level. Indeed, the Federal Trade Commission recently announced a $5 billion settlement after the company violated an existing consent decree. Facebook's delays and refusals to comply with the Attorney General's interrogatories and subpoena should not thwart this important and independent investigation into whether the company violated its users' privacy and California law.

THE PARTIES

5. Petitioner Xavier Becerra is the Attorney General of the State of California. He brings this action solely in his official capacity on behalf of the People of the State of California. As the chief law officer of the State of California, the Attorney General is responsible for enforcing the

state's consumer protection laws, among others. In order to carry out these duties effectively, California law gives the Attorney General broad investigative powers. Specifically, Government Code sections 11180 *et seq.* grant the Attorney General, as head of the Department of Justice, the authority to issue subpoenas and promulgate interrogatories. The Attorney General may use these powers for various reasons, including assisting him in considering possible prosecutorial actions, proposing legislation, and formulating enforcement policies with other agencies. These investigative powers are not dependent on the initiation of a civil lawsuit or an administrative proceeding. If a party disobeys a subpoena, the Attorney General may petition the Superior Court for enforcement.

6. Facebook needs no introduction. The Silicon Valley-based social media giant, which has grown to include the Facebook, WhatsApp, and Instagram platforms, is the fifth largest company in the United States by market capitalization, sixth most profitable, and boasts nearly 40,000 employees. Most adults with internet access use Facebook, many of them to share the intimate details of their lives with friends and family. Facebook gathers and maintains personal information of billions of users throughout the world and millions in California. This data gathering occurs both on Facebook's own platforms and through widespread surveillance that Facebook conducts on other websites and online activities. The company then monetizes the data through the provision of highly targeted advertisements to customized audiences on Facebook's products, making the company billions in revenue.

JURISDICTION AND VENUE

7. Jurisdiction and venue are proper in the Superior Court of the State of California in the City and County of San Francisco under Government Code section 11186. The Attorney General primarily conducts the investigation into Facebook in the City and County of San Francisco, with some work performed in other parts of the State.

BACKGROUND

I. THE FACEBOOK PLATFORM

8. Among other endeavors, Facebook operates a social media platform that allows individuals and organizations to create personalized online profile pages about themselves, filled

with biographical details, photos, and a scrollable record of chronological "posts" about the user. Facebook also lets users connect with other users as "Friends," and as relevant here, purports to allow users to restrict access to their information using various privacy settings.

9. In 2007, Facebook launched a developer portal that let third-party software developers create applications that interacted with Facebook users. These "Facebook apps," like apps on a mobile phone, were small programs that operated on Facebook's website or mobile app. Facebook apps included popular games or quizzes that allowed a user to post serious or humorous results, such as what fictional character a user's personality resembles. To make them personalized, Facebook granted apps the ability to access data about users from Facebook's database. For example, a horoscope app might capture a user's birthdate to provide the horoscope. Facebook made millions of apps available to users, opening the door for millions of apps to collect user data.

10. Facebook also allowed apps to access non-public data—information that users thought they had restricted—about both themselves and their Friends. Some app providers, appear to have exploited this access to collect other user data, build profiles on users, and sell those to third parties. This includes apps affiliated with Cambridge Analytica, which obtained data on 87 million Americans that was allegedly used to conduct election-related disinformation campaigns. Questions have arisen as to what Facebook knew about this conduct, why it failed to prevent app providers from misusing user data, and whether this behavior violated California law.

11. In addition, Facebook told users that the company had safeguards in place to protect their data, and it offered controls that purported to allow users to decide whether and how their data was shared. However, the Cambridge Analytica scandal, combined with reports that Facebook allowed its business partners to access user data, even when those users had opted out of such sharing, suggests that Facebook may not have honored its obligations to its users, or complied with California's privacy or consumer protection laws.

II. THE ATTORNEY GENERAL'S INVESTIGATION

12. California law grants the Attorney General the authority to investigate reports of unlawful, unfair, deceptive, or otherwise improper business practices, including

misrepresentations to consumers, failures to make adequate disclosures in connection with personal information and online services, and violations of individuals' privacy. Using this authority, the Attorney General initiated an investigation and continues to investigate Facebook's compliance with California's privacy and consumer protection laws, including but not limited to the allegations set forth above.

13. On June 4, 2018, the Attorney General, acting through officers of the Department of Justice to whom he had delegated investigative authority under section 11182 of the Government Code, served Facebook with a subpoena for documents based on the allegations involving Facebook and Cambridge Analytica. Facebook accepted service of the subpoena and acknowledged its receipt. Facebook made its last production of documents in response to this first subpoena on April 17, 2019, but the company wrote that it planned to make additional productions "on a rolling basis." On June 5, 2019, a year and a day after the subpoena issued, Facebook finally admitted that it had actually completed its production of documents.

14. On June 17, 2019, the Attorney General, acting through officers of the Department of Justice exercising delegated authority, properly served Facebook with a second set of investigative interrogatories and a second investigative subpoena, requesting additional information and documents. Copies of the investigative interrogatories and subpoena are attached as Exhibit A and B and are incorporated into this petition. Facebook was subpoenaed and required to answer interrogatories in the manner prescribed in section 11180 *et seq.* of the Government Code. The interrogatories and the subpoena, respectively, provided notice of the time and place for answering the interrogatories and for production of the papers. (Gov. Code, § 11187, subd. (b)(1).) By agreement, Facebook's attorneys accepted service of the interrogatories and subpoena.

15. The Attorney General's interrogatories and subpoena were regularly issued, and they relate to the Attorney General's ongoing investigation into Facebook's compliance with consumer protection and privacy laws. The investigatory interrogatories seek the following relevant information:

- The number of California users and rates at which they activated privacy settings to

prevent apps from accessing data;

- The effects of the various privacy settings on third parties' access to data, including which apps Facebook granted access to user data despite users restricting access to their information;
- Information about Facebook's enforcement of its policies against developers;
- An explanation of the technical workings of Facebook's software that allowed various entities to access user data.

The Attorney General's subpoena seeks the following materials:

- Communications among executives regarding: 1) any consideration of the need to audit developers' access to user data; 2) third parties granted expanded access to user data; 3) the relationship between ad spending and access to data; 4) significant privacy-related news stories; and 5) the introduction of new privacy features.
- Documentation regarding the changes to and user testing of Facebook's privacy settings;
- Communications regarding a user's likely response to privacy settings;
- Documents regarding Facebook's privacy program, which was mandated by the Federal Trade Commission in 2012 pursuant to a consent decree, yet failed to prevent the Cambridge Analytica scandal.

III. FACEBOOK HAS FAILED TO ADEQUATELY AND SUBSTANTIVELY RESPOND.

16. Facebook broadly refuses to answer the interrogatories or comply with the subpoena as required. Facebook will not provide a direct answer to 19 out of 27 interrogatories (Nos. 26-37, 40-42, & 47-50) and has only provided a partial response to 6 (Nos. 24, 25, 43, 44, 45, & 46). Facebook has produced no new documents for six document requests (Nos. 19-21 & 26-28), and appears to have conducted an insufficient search for request no. 25.

17. Facebook has also refused to conduct a complete search for responsive documents. Facebook has, for example, refused to search for communications among senior executives regarding terminating developers' access to user data, various privacy-related news stories, and Facebook's public responses. On information and belief, Facebook has not searched the emails of the company's Chief Executive and Chief Operating Officers for documents responsive to the

subpoena.

18. This lack of cooperation, particularly with respect to communications among senior executives, is not unique to the Attorney General's investigation. A member of the Federal Trade Commission recently wrote to express serious concerns over Facebook's candor with federal regulators:

> Based on the material presented to me, I was very concerned about Facebook's cooperation and candor in its dealings with the Commission and its staff. In my view, there were multiple inconsistencies and deficiencies in Facebook's responses to questions. I questioned whether the company's document productions were truly complete. I believe that Facebook struggled to answer many requests for data, and I ascertained that the company was resistant to providing documents from Zuckerberg's files.

(Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.*, Federal Trade Commission File No. 1823109, July 24, 2019, at page 6.)

///

PRAYER FOR RELIEF

Pursuant to Government Code sections 11186-11188, the Attorney General prays that this Court:

1. Issue an order directing Respondent to appear before this Court and to show cause why it has refused to comply with the Subpoena and Interrogatories, and, upon Respondent's failure to show cause;

2. Enter an order directing Respondent to provide full responses to Interrogatories Nos. 26 – 37, 40 – 42, and 47-50; complete its response to Interrogatories Nos. 24, 25, 43, 44, 45, & 46; and produce documents for Requests for Production Nos. 19-21 and 25-28; and

3. All other relief to which the people are legally entitled.

Dated: November 6, 2019

Respectfully Submitted,

XAVIER BECERRA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER
Supervising Deputy Attorney General

MICAH C. E. OSGOOD
LISA B. KIM
SUSAN SAYLOR
MANEESH SHARMA
Deputy Attorneys General
Attorneys for the People of the State of California

SF2018400570/14237593.docx

EXHIBIT A

XAVIER BECERRA (SBN 118517)
Attorney General of California
NICKLAS A. AKERS (SBN 211222)
Senior Assistant Attorney General
STACEY D. SCHESSER (SBN 245735)
Supervising Deputy Attorney General
LISA B. KIM (SBN 229369)
SUSAN SAYLOR (SBN 154592)
MICAH C.E. OSGOOD (SBN 255239)
MANEESH SHARMA (SBN 280084)
Deputy Attorneys General
300 South Spring Street, Suite 1702
Los Angeles, CA 90013
Telephone: (213) 269-6369
lisa.kim@doj.ca.gov

BEFORE THE DEPARTMENT OF JUSTICE

OFFICE OF THE ATTORNEY GENERAL

STATE OF CALIFORNIA

In the Matter of the Investigation of: **FACEBOOK, INC.**	**INVESTIGATIVE SUBPOENA FOR DOCUMENTS [SET TWO]** GOV. CODE § 11180, ET SEQ.

NOTICE to Benjamin A. Powell, Esq.: You are hereby served on behalf of Facebook, Inc. pursuant to your agreement to accept service on your client's behalf.

Pursuant to the powers conferred by Article 2 of Chapter 2 of Division 3 of Title 2 of the Government Code of California (Cal. Gov. Code, § 11180 et seq.) on the Attorney General, as head of the California Department of Justice, which powers and authority to conduct the above entitled investigation have been delegated to the undersigned, an officer of that Department,

FACEBOOK, INC.

(hereinafter "FACEBOOK") IS HEREBY COMMANDED to produce the documents, books, records, papers and other items (collectively "Items") described in Attachment A to this Investigative Subpoena which are in FACEBOOK's custody, possession or control, or the custody, possession or control of FACEBOOK's subsidiaries, affiliates, parents, predecessors, successors, employees, partners, officers, agents or representatives, whether or not the present location of any of the Items designated is in California, at the California Department of Justice, Office of the Attorney General, 1300 "I" Street, Sacramento, CA 95814-2919, ATTN: Deputy Attorney General Lisa B. Kim, within thirty days of service hereof.

INSTRUCTIONS FOR COMPLIANCE

1. If FACEBOOK claims that an item or a portion of an item is privileged and FACEBOOK withholds it from production for that reason, FACEBOOK must create and submit a privilege log which lists: (1) the authors and their capacities; (2) the recipients (including cc's and bcc's) and their capacities; (3) other individuals with access to the document and their capacities; (4) the type of document; (5) the subject matter of the document; (6) the purpose(s) for the creation of the document; (7) the date on the document; and (8) a detailed explanation setting forth the factual and legal basis for your claim that the document is privileged or otherwise immune from production.

2. To the extent responsive items exist in an electronic or computerized format, please contact the officer issuing this subpoena to discuss the manner and format in which the items are to be produced so as to facilitate the production of full and complete copies in a usable format. In the absence of an agreement regarding the manner and format of production, the following instructions shall apply:

a. The information shall be provided in accordance with the California Attorney General's Office Production Format as outlined in Attachment B below.

b. The response shall include all DOCUMENTS and computer programs necessary to the accurate conversion, analysis, and review of the electronic data, including but not limited to operating instructions, manuals and user guides, keys, legends, and codes for systems, programs, files, and data fields.

3. This Investigative Subpoena has been issued in connection with an investigation within the scope of section 131 of the California Penal Code.

4. No item requested herein shall be destroyed or discarded by FACEBOOK until the Attorney General has made a written determination that the item in question is not necessary for furtherance of this investigation.

5. When producing items, identify by number the request(s) to which the Item is responsive.

6. As used herein, the past tense includes the present and future tenses, the present tense includes the past and future tenses, and the future tense includes the past and present tenses; tenses must be construed in the manner that would include, rather than exclude, information.

7. As used herein, the singular includes the plural and the plural includes the singular, and must be construed in the manner that would include, rather than exclude, information.

DEFINITIONS

For purposes of this investigative subpoena, the terms set forth below are defined as follows:

1. "APPS OTHERS USE" means the setting used to limit data SHARED through FRIENDS with THIRD PARTY APPLICATIONS as set out on page 19 et seq. of the March 15, 2019 letter from Benjamin A. Powell to Stacey D. Schesser and Lisa B. Kim.

2. "COMMUNICATION(S)" means every disclosure, transfer, exchange, OR transmission of information, whether oral, written, OR electronic, and whether face-to-face, by telecommunications, telephone, computer, mail, e-mail, text message, instant message,

FACEBOOK Messenger, screenshot, picture, facsimile (fax) machine, OR otherwise, including any and all attachment(s).

3. "DATA CONTROLS" means the settings that a user can alter or accept to limit the sharing of USER INFORMATION with third parties, including audience selectors, GRANULAR DATA PERMISSIONS, PLATFORM OPT OUT, APPS OTHERS USE, and the like.

4. "DEVELOPER(S)" means any natural or corporate person that develops an application, software experience, game, or website, that accesses information from FACEBOOK's APIs or other FACEBOOK software.

5. "DOCUMENT(S)" means a "writing" as defined in section 250 of the California Evidence Code, and includes COMMUNICATIONS, e-mails, voicemails, computer files, text messages, instant messages, word processing documents, spreadsheets, databases, calendars, and all other forms of "electronically stored information" as defined in section 2016.020 of the California Code of Civil Procedure.

6. "EXTENDED API ACCESS PARTNER(S)" means the entity or entities with whom FACEBOOK partnered with for EXTENDED API ACCESS PARTNERSHIPS.

7. "EXTENDED API ACCESS PARTNERSHIP" means a partnership formed by agreement between FACEBOOK and a DEVELOPER that allowed the DEVELOPER access to certain FACEBOOK APIs on terms specified within the agreement, such as FB-CA-CAAG-0002916, and beyond those terms offered to typical THIRD PARTY APPLICATIONS on the FACEBOOK Platform. This definition includes agreements performing the same general function, even if not titled as an "Extended API Addendum."

8. "FACEBOOK PRODUCT" means the social networking online service operated by FACEBOOK, Inc. where USERS access content, including THIRD PARTY APPLICATIONS, websites, and games. For purposes of this subpoena, FACEBOOK PRODUCT means content accessed online at www.facebook.com and FACEBOOK's mobile application, but does not include acquired properties, such as Instagram and WhatsApp.

9. "FRIEND" means a USER who is connected to another USER on the FACEBOOK PRODUCT.

10. "GRANULAR DATA PERMISSIONS" refers to the setting used to limit data SHARED with THIRD PARTY APPLICATIONS as set out at page 4 *et seq.* of the March 15, 2019 letter from Benjamin A. Powell to Stacey D. Schesser and Lisa B. Kim.

11. "INSTANT PERSONALIZATION" means the product that FACEBOOK offered that used FACEBOOK USER INFORMATION to provide personalized experiences on select partners' websites, as described by FACEBOOK in its December 18, 2018 Newsroom post found online at https://newsroom.fb.com/news/2018/12/facebooks-partners/.

12. "INSTANT PERSONALIZATION PARTNER(S)" means the entity or entities with whom FACEBOOK partnered for INSTANT PERSONALIZATION.

13. "INSTANT PERSONALIZATION PARTNERSHIP" means the relationship FACEBOOK had with INSTANT PERSONALIZATION PARTNERS.

14. "INTEGRATION PARTNER(S)" means the entity or entities with whom FACEBOOK has an INTEGRATION PARTNERSHIP.

15. "INTEGRATION PARTNERSHIP(S)" means the relationship FACEBOOK has with companies that built integrations for a variety of devices, operating systems, and other products, as described by FACEBOOK in Appendix A of the July 20, 2018 letter Anjan Sahni sent to Stacey D. Schesser and Lisa B. Kim.

16. "PLATFORM OPT OUT" means the setting used to disable platform as set out at page 10 et seq. of the March 15, 2019 letter from Benjamin A. Powell to Stacey D. Schesser and Lisa B. Kim.

17. "POLICY" or "POLICIES" mean any formal or informal policy, procedure, rule, guideline, collaborative document, directive, instruction, OR practice, whether written or unwritten, that YOU expect YOUR employees to follow in performing their jobs.

18. "PROFILE CONTROLS" means the settings that control what information in a USER's profile is SHARED with other USERS through audience selectors, such as phone number, email, current city, birthday, relationship status, work, and education.

19. "SHARE" or "SHARES" or "SHARING" or "SHARED" means to provide, communicate, transfer, release, disclose, disseminate, sell, rent, trade, OR otherwise make accessible or available in writing, electronically, or by other means.

20. "THIRD PARTY APPLICATION(S)" shall have the same meaning as the terms "Platform Application(s)," "application(s)," and "app" used in FACEBOOK's policies produced to the California Attorney General bearing the Bates Labels FB-AG-00000001 through FB-CA-CAAG-00000305.

21. "USER(S)" means the individuals who maintain an account and can generally access the typical FACEBOOK experience via website or mobile application in a personal capacity.

22. "USER INFORMATION" means any information related to the FACEBOOK PRODUCT that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, the following information: name; physical address, including street name and name of a city or town; telephone number; email address; online contact information, including a screen name, username, or social network profile that functions as online contact information; user account credentials; a persistent identifier such as a user number held in a cookie or a processor serial number; a unique device identifier or a universally unique identifier, including FBID; geolocation information, including GPS-based location information and network-based or cell-based location information; longitude and latitude data; education; employment; employment history; and any other social media content generated by OR associated with a particular individual; including status updates, likes, OR group affiliations.

23. "YOU" or "YOUR" or "FACEBOOK" means FACEBOOK, Inc. and its past or present officers, agents, employees, attorneys, predecessors, affiliates, subsidiaries, parent

///

///

///

///

///

companies, former business names, and dbas, and anyone acting on YOUR behalf or at YOUR direction.

FAILURE TO COMPLY WITH THIS SUBPOENA WILL SUBJECT YOU TO THE PROCEEDINGS AND PENALTIES PROVIDED BY LAW.

Dated: June 17, 2019

XAVIER BECERRA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER
Supervising Deputy Attorney General
LISA B. KIM
SUSAN SAYLOR
MICAH C.E. OSGOOD
MANEESH SHARMA
Deputy Attorneys General

LISA B. KIM
Deputy Attorney General

SF2017402454
13780166.docx

ATTACHMENT A

18. Records tracking the USER DATA access permissions granted to DEVELOPERS pursuant to an EXTENDED API ACCESS PARTNERSHIP.

19. All YOUR internal COMMUNICATIONS from 2013 to 2018 reflecting the contemplation, planning, or performance of a general audit of DEVELOPERS' access to USER INFORMATION, including through THIRD PARTY APPLICATIONS, INTEGRATION PARTNERSHIPS, INSTANT PERSONALIZATION PARTNERSHIPS, and EXTENDED API ACCESS PARTNERSHIPS.

20. All COMMUNICATIONS concerning the negotiation of, entrance into, or termination of, an EXTENDED API ACCESS PARTNERSHIP.

21. All COMMUNICATIONS from 2012 to 2015 regarding conditioning DEVELOPERS' access to USER INFORMATION on advertising spending or other payment.

22. All DOCUMENTS that support YOUR contention that FACEBOOK "*never implemented*, let alone seriously considered" (emphasis in the original) "charging developers for access to user data," as stated on page 6 of the April 17, 2019 letter from Benjamin A. Powell to Stacey D. Schesser and Lisa B. Kim.

23. All DOCUMENTS reflecting the study, testing, or analysis of a USER'S understanding of, or reaction to, a DATA CONTROL in effect during 2013 to present, or any proposed change to a DATA CONTROLS during that time frame, including any A/B testing, or studies on user experience or usability of DATA CONTROLS.

24. All COMMUNICATIONS regarding a USER's potential reaction to or understanding of DATA CONTROLS.

25. All YOUR internal COMMUNICATIONS, involving a Director, Vice President, or above, about the development of the "privacy tour," "privacy basics," or "privacy check-up," as those terms were used by in the March 15, 2019 letter from Benjamin A. Powell to Stacey D. Schesser and Lisa B. Kim.

26. All YOUR internal COMMUNICATIONS, involving a Director, Vice President, or above, about the termination of a DEVELOPER'S access to USER INFORMATION.

27. All YOUR internal COMMUNICATIONS, involving a Director, Vice President, or above, that occurred within one week of a request for comment regarding, or the publication of, the following news reports:

- *The Guardian's* reporting on December 11, 2015, that "Ted Cruz us[ed] [a] firm that harvested data on millions of unwitting Facebook users";
- Various news outlets reporting on March 17, 2018, about Facebook and Cambridge Analytica;
- *The New York Times* reporting on June 3, 2018, that "Facebook gave device makers deep access to data on users and friends";
- *The Wall Street Journal* reporting on November 28, 2018, that "Facebook considered charging for access to user data";
- *The Washington Post* reporting on December 5, 2018, that "Facebook [allegedly] offered advertisers special access to users' data and activities"; and
- *The New York Times* reporting on December 18, 2018, that "Facebook gave some of the world's largest technology companies more intrusive access to users' personal data."

28. All YOUR internal COMMUNICATIONS, involving a Director, Vice President, or above, regarding approval of the following Facebook Newsroom items:

- Why We Disagree with the New York Times, dated June 3, 2018;
- Response to Six4Three Documents, dated December 5, 2018
- Let's Clear Up a Few Things About Facebook's Partners, dated December 18, 2018.
- Facts About Facebook's Messaging Partnerships, dated December 19, 2018;
- Cracking Down on Platform Abuse, dated March 21, 2018;

29. All YOUR internal POLICIES on the enforcement of FACEBOOK's Platform Policy, Data Policy, Terms of Service, or Statement of Rights and Responsibilities, on THIRD PARTY APPLICATIONS, INTEGRATION PARTNERSHIPS, INSTANT PERSONALIZATION PARTNERSHIPS, and EXTENDED API ACCESS PARTNERSHIPS.

30. All "Enforcement Rubric[s]" used by FACEBOOK, as that term is used on page 4 of the April 17, 2019 letter from Benjamin A. Powell to Stacey D. Schesser and Lisa B. Kim.

31. All "cease and desist letters" sent by FACEBOOK to DEVELOPERS, between January 1, 2013, and March 1, 2018, as that term is used on page 12 of the July 20, 2018 letter from Anjan Sahni to Stacey D. Schesser and Lisa B. Kim.

32. All "letter agreements" resolving an enforcement concern as that term is used on page 12 of the July 20, 2018 letter from Anjan Sahni to Stacey D. Schesser and Lisa B. Kim.

33. FACEBOOK'S logs documenting any code changes made to DATA CONTROLS, sometimes referred to as "Commit Logs."

34. All "Privacy Risk Assessment[s]," and notes or agenda relating to FACEBOOK's "focused subject-matter-specific meetings," "weekly intra- and inter-team meetings," and "Privacy Summit[s]," as detailed in "Facebook's Privacy Program Overview" at page 9 of the "Independent Assessor's Report on Facebook's Privacy Program" at FB-CA-CAAG-00131372.

35. All transcripts of deposition or other testimony by FACEBOOK former and current employees in the litigation titled, *Six4Three, LLC v. Facebook, Inc.* (Case No. CIV 533328), Superior Court of the State of California, County of San Mateo, filed on April 10, 2015.

36. FACEBOOK's discovery responses, excluding documents produced, in the litigation titled, *Six4Three, LLC v. Facebook, Inc.* (Case No. CIV 533328), Superior Court of the State of California, County of San Mateo, filed on April 10, 2015.

37. FACEBOOK's responses to any formal or informal requests for information, interrogatories, or other discovery, excluding documents produced, to the Federal Trade Commission regarding its investigation into FACEBOOK's privacy practices, after entry of the Federal Trade Commission's July 27, 2012 Decision and Order, in its action titled In the Matter of Facebook, Inc. Doc. No. 0923184.

ATTACHMENT B

California Attorney General's Office

PRODUCTION FORMAT

I. PRODUCTION OF ELECTRONICALLY STORED INFORMATION (ESI)

A. Load files. Except where noted in section (K) below, all ESI is to be produced in electronic format, with file suitable for loading into a Concordance compatible litigation support review database. All productions will include both image and metadata load files, as described in Appendix A: Load File Format.

B. Metadata Fields and Processing. Each of the metadata and coding fields set forth in Appendix B that can be extracted from a document shall be produced for that document. The parties are not obligated to populate manually any of the fields in Appendix B if such fields cannot be extracted from a document.

C. System Files. Common system and program files need not be processed, reviewed or produced. The producing party shall keep an inventory of the system files not being produced and the criteria *(e.g.,* non-human readable file, etc.) for not processing the files.

D. Email. Whenever possible, email shall be collected from the producing party's email store or server *(e.g.,* MS Exchange, Lotus Notes) because this is the most reliable source from which to produce and maintain email metadata and structure. Metadata and "header fields" shall be extracted from email messages. Email messages, meeting notices, calendar items, contacts and tasks shall all be extracted from the email archives.

E. De-Duplication. Removal of duplicate documents shall only be done on exact duplicate documents (based on MD5 or SHA-1 hash values at the document level) *across all custodians* (global), and the Custodian field will list each Custodian, separated by a semicolon, who was a source of that document prior to deduplication. If a party is unable to provide such information within the Custodian field, or if global deduplication could otherwise limit the ability to provide that a particular document was possessed by a custodian, then removal of duplicate documents shall only be done on exact duplicate documents (based on MD5 or SHA-1 hash values at the document level) *within a source* (custodian).

F. TIFFs/JPGs. Single-page Group IV TIFF images shall be provided using at least 300 DPI print setting. Each image shall have a unique file name, which is the Bates number of the document. Original document orientation shall be maintained *(i.e.,* portrait to portrait and landscape to landscape). TIFFs will show any and all text and images which would be visible to the reader using the native software that created the document. Documents containing color need not be produced initially in color. However, if an original document contains color necessary to understand the meaning or content of the document, the producing party will honor reasonable requests for a color image of the document. If color images are to be produced, they will be provided in JPG format.

G. Embedded Objects. Objects embedded in Microsoft Word and .RTF documents, which have been embedded with the "Display as Icon" feature, will be extracted as separate documents and treated like attachments to the document. Other objects embedded in documents shall be produced as native files.

H. Compressed files. Compression file types (*e.g.*, .CAB, .GZ, .TAR, .Z, .ZIP) shall be decompressed in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual folders and/or files.

I. Text Files. For each document, a single text file shall be provided along with the image files and metadata. The text file name shall be the same as the page Bates/control number of the first page of the document. File names shall not have any special characters or embedded spaces. Electronic text must be extracted directly from the native electronic file unless the document was redacted, an image file, or a physical file. In these instances a text file created using OCR will be produced in lieu of extracted text. See Section II.C for OCR requirements. Under no circumstances shall the receiving party be required to rely upon a less accurate version of the text than the producing party. For example, if the producing party has access to extracted text from electronic document files, the receiving party shall receive extracted text instead of OCR'd text generated from an image file.

J. Redaction. If a file that originates in ESI needs to be redacted before production, the file will be rendered in TIFF, and the TIFF will be redacted and produced. However, to the extent that the text is searchable in the native format, the producing party will still provide searchable text for those portions of the document that have not been redacted.

K. Spreadsheets and Presentations. Various types of files, including but not limited to MS Excel spreadsheets, MS PowerPoint presentations, media files, etc., lose significant information and meaning when produced as an image. Any native files that are produced shall be produced with a Bates-numbered TIFF image slip-sheet stating the document has been produced in native format. Any native files that are produced shall be produced with the Source File Path provided, as well as all extracted text and applicable metadata fields set forth in Appendix B.

- Spreadsheets. Excel spreadsheets shall be produced as a native document file along with the extracted text and relevant metadata identified in Appendix B for the entire spreadsheet, plus a Bates-numbered TIFF image slip-sheet stating the document has been produced in native format.

- Presentations. PowerPoint presentations shall be produced as a native document file along with the extracted text and relevant metadata identified in Appendix B for the entire presentation, plus a Bates-numbered TIFF image slip-sheet stating the document has been produced in native format.

L. Other ESI that is Impractical to Produce in Traditional Formats. The parties understand and acknowledge that certain categories of ESI are structurally complex and do not lend themselves to production as native format or other traditional formats. To the extent a response to discovery requires production of discoverable electronic information contained in a database, the producing party shall consider methods of production best providing all relevant information, including but not limited to duplication of databases or limited access for the purpose of generating reports. Parties should consider whether all relevant information may be provided by querying the database for discoverable information and generating a report in a reasonably usable and exportable electronic file (*e.g.*, Excel, CSV or SQL format). The parties agree to confer to obtain an appropriate resolution to such requests.

M. Endorsements. The producing party will brand all TIFF images in the lower right-hand corner with its corresponding bates number, using a consistent font type and size. The bates number must not obscure any part of the underlying data. The producing party will brand all TIFF images in the lower left-hand corner with all confidentiality designations, as needed, in accordance with confidentiality definitions as agreed to by the parties.

N. Exception Report. The producing party shall compile an exception report enumerating any unprocessed or unprocessable documents, their file type and the file location.

O. Clawback procedure. Any documents recalled due to a mutually-agreed upon clawback provision shall have a specific protocol followed to ensure all copies of each such document are appropriately removed from the review database, backup and disaster recovery systems maintained by the opposing party.

II. PRODUCTION OF PHYSICALLY STORED INFORMATION (HARD COPY DOCUMENTS)

A. TIFFs. Hard copy paper documents shall be scanned as single-page, Group IV compression TIFF images using a print setting of at least 300 dots per inch (DPI). Each image shall have a unique file name, which is the Bates number of the document. Original document orientation shall be maintained *(i.e.,* portrait to portrait and landscape to landscape).

B. Metadata Fields. The following information shall be produced for hard copy documents and provided in the data load file at the same time that the TIFF images and the Optical Character Recognition (OCR) acquired text files are produced. Each metadata field shall be labeled as listed below:

Field Name	Example / Format	Description
PARENTDOCID	ABC0000001 (Unique ID Parent-Child Relationships)	The Document ID number associated with the first page of a parent document (this field will only be populated in child records).
GROUPID	ABC0000001 (Unique ID Parent-Child Relationships)	The Document ID number associated with the first page of the parent document (in most cases, this will be data in the BEGATTACH field).
BEGBATES	ABC0000001 (Unique ID)	The Document ID number associated with the first page of a document.
ENDBATES	ABC0000003 (Unique ID)	The Document ID number associated with the last page of a document.
BEGATTACH	ABC0000001 (Unique ID Parent-Child Relationships)	The Document ID number associated with the first page of the parent document (if applicable).
ENDATTACH	ABC0000008 (Unique ID Parent-Child Relationships)	The Document ID number associated with the last page of the last attachment (if applicable).
PGCOUNT	3 (Numeric)	The number of pages for a document.
VOLUME	VOL001	The name of CD, DVD or Hard Drive (vendor assigns).
CUSTODIAN		The custodian / source of a document. Note: If the documents are de-duped on a global level, this field will contain the name of each custodian from which the document originated.

C. OCR Acquired Text Files. When subjecting physical documents to an OCR process, the settings of the OCR software shall maximize text quality over process speed. Any settings such as "auto-skewing", "auto-rotation" and the like should be turned on when documents are run through the process.

D. Database Load Files/Cross-Reference Files. Documents shall be provided with (a) a delimited metadata file (.dat or .txt) and (b) an image load file (.opt), as detailed in Appendix A.

F. Unitizing of Documents. In scanning paper documents, distinct documents shall not be merged into a single record, and single documents shall not be split into multiple records *(e.g.,* paper documents should be logically unitized). In the case of an organized compilation of separate documents - for example, a binder containing several separate documents behind numbered tabs - the document behind each tab should be scanned separately, but the relationship among the documents in the binder should be reflected in proper coding of the beginning and ending document and attachment fields. The parties will make their best efforts to unitize documents correctly.

APPENDIX A: REQUESTED LOAD FILE FORMAT FOR ESI

1. Image File Format: All images, paper documents scanned to images or rendered ESI, shall be produced as 300 dpi single-page, CCITT Group IV TIFF images (for black/white) or JPG images (for color). Documents should be uniquely and sequentially Bates numbered with an endorsement burned into each image.

- All TIFF/JPG image file names shall include the unique Bates number burned into the image.
- Each Bates number shall be a standard length, include leading zeros in the number and be unique for each produced page.
- All TIFF/JPG image files shall be named with a ".tif" or ".jpg" extension.
- Images should be able to be OCR'd using standard COTS products, such as LexisNexis LAW PreDiscovery, Ipro, etc.

2. Concordance Image Cross-Reference file: Images shall be accompanied by a Concordance Image Cross-Reference file that associates each Bates number with its corresponding single-page TIFF/JPG image file. The Cross-Reference file should also contain the image file path for each Bates numbered page.

- Image Cross-Reference Sample Format:
  ABC000001,OLS,D:\DatabaseName\Image\001\ABC000001.TIF,Y,,,
  ABC000002,OLS,D:\DatabaseName\Image\001\ABC000002.TIF,,,,
  ABC000003,OLS,D:\DatabaseName\Image\001\ABC000003.TIF,,,,
  ABC000004,OLS,D:\DatabaseName\Image\001\ABC000004.TIF,Y,,,

3. Concordance Load File: Images shall also be accompanied by a "text load file" containing delimited text (DAT file) that will populate fields in a searchable, flat database environment. The delimiters for the load file should be Concordance defaults.

- Comma: ¶ ASCII character (020)
- Quote: þ ASCII character (254)
- Newline: ® ASCII character (174)

APPENDIX B: REQUESTED METADATA FIELDS FOR ESI

Field Name	Example / Format	Description
PARENTDOCID	ABC0000001 (Unique ID Parent-Child Relationships)	The Document ID number associated with the first page of a parent document (this field will only be populated in child records).
GROUPID	ABC0000001 (Unique ID Parent-Child Relationships)	The Document ID number associated with the first page of the parent document (in most cases, this will be data in the BEGATTACH field).
BEGBATES	ABC0000001 (Unique ID)	The Document ID number associated with the first page of a document.
ENDBATES	ABC0000003 (Unique ID)	The Document ID number associated with the last page of a document.
BEGATTACH	ABC0000001 (Unique ID Parent-Child Relationships)	The Document ID number associated with the first page of the parent document.
ENDATTACH	ABC0000008 (Unique ID Parent-Child Relationships)	The Document ID number associated with the last page of the last attachment.
PGCOUNT	3 (Numeric)	The number of pages for a document.
VOLUME	VOL001	The name of CD, DVD or Hard Drive (vendor assigns).
SENTDATE	MM/DD/YYYY	The date the email was sent. **NOTE:** For attachments to e-mails, this field should be populated with the date sent of the email transmitting the attachment.
SENTTIME	HH:MM:SS	The time the email was sent.
CREATEDATE	MM/DD/YYYY	The date the document was created.
CREATETIME	HH:MM:SS	The time the document was created.
LASTMODDATE	MM/DD/YYYY	The date the document was last modified.
LASTMODTIME	HH:MM:SS	The time the document was last modified
RECEIVEDDATE	MM/DD/YYYY	The date the document was received.
RECEIVEDTIME	HH:MM:SS	The time the document was received.
FILEPATH	i.e. Joe Smith/E-mail/Inbox Joe Smith/E-mail/Deleted Items Joe Smith/Loose Files/Accounting/... Joe Smith/Loose Files/Documents and Settings/...	Location of the original document. The source should be the start of the full path.
APPLICATION	MS Word, MS Excel, etc.	Type of document by application.
HIDDENTYPE	Options: Track Changes, Hidden Spreadsheet, Very Hidden Spreadsheet, etc.	The type of hidden modification of the document (e.g. Track Changes, Hidden Spreadsheet, Very Hidden Spreadsheet, etc)
AUTHOR	jsmith	The author of a document from entered metadata.

Field Name	Example / Format	Description
FROM	Joe Smith <jsmith@email.com>	The display name and e-mail of the author of an e-mail. If only e-mail is given, then just list the e-mail address. An e-mail address should always be provided for every document.
TO	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and e-mail of the recipient(s) of an e-mail. If only e-mail is given, then just list the e-mail address. An e-mail address should always be provided for every document.
CC	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and e-mail of the copyee(s) of an e-mail. If only e-mail is given, then just list the e-mail address. An e-mail address should always be provided for every document.
BCC	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and e-mail of the blind copyee(s) of an e-mail. If only e-mail is given, then just list the e-mail address. An e-mail address should always be provided for every document.
ESUBJECT	Re: Scheduling Meet and Confer	The email subject line.
DOCTITLE		The extracted document title or subject of a document.
CUSTODIAN		The custodian / source of a document. Note: If the documents are de-duped on a global level, this field will contain the name of each custodian from which the document originated.
ATTACH COUNT	Numeric	The number of attachments to a document.
FILEEXT	XLS	The file extension of a document.
FILENAME	Document Name.xls	The file name of a document.
HASH		The MD5 or SHA-1 Hash value.
NATIVELINK	D:\NATIVES\ABC000001.xls	The full path to a native copy of a document.
FULLTEXT	D:\TEXT\ABC000001.txt	The path to the full extracted text of the document. There should be a folder on the deliverable, containing a separate Unicode text file per document. These text files should be named with their bates numbers. Note: E-mails should include header information: author, recipient, cc, bcc, date, subject, etc. If the attachment or e-file does not extract any text, then OCR for the document should be provided.

DECLARATION OF SERVICE BY E-MAIL

Matter Name: In the Matter of the Investigation of: FACEBOOK, INC.

I declare:

I am employed in the Office of the Attorney General, which is the office of a member of the California State Bar, at which member's direction this service is made. I am 18 years of age or older and not a party to this matter; my business address is 300 South Spring Street, Suite 1702, Los Angeles, CA 90013.

On June 17, 2019, I served the attached **INVESTIGATIVE SUBPOENA FOR DOCUMENTS [SET TWO]** by placing a true copy thereof enclosed in a sealed envelope with postage thereon fully prepaid, in the United States Mail at Los Angeles, California, addressed as follows:

Benjamin A. Powell
Maury Riggan
WilmerHale
1875 Pennsylvania Avenue NW
Washington, DC 20006
Benjamin.Powell@wilmerhale.com
Maury.Riggan@wilmerhale.com

I declare under penalty of perjury under the laws of the State of California the foregoing is true and correct and that this declaration was executed on June 17, 2019, at Los Angeles, California.

Carol Chow
Declarant

Signature

SF2018400570
53504639.docx

Exhibit B

XAVIER BECERRA (SBN 118517)
Attorney General of California
NICKLAS A. AKERS (SBN 211222)
Senior Assistant Attorney General
STACEY D. SCHESSER (SBN 245735)
Supervising Deputy Attorney General
LISA B. KIM (SBN 229369)
SUSAN SAYLOR (SBN 154592)
MICAH C.E. OSGOOD (SBN 255239)
MANEESH SHARMA (SBN 280084)
Deputy Attorneys General
300 South Spring Street, Suite 1702
Los Angeles, CA 90013
Telephone: (213) 269-6369
Lisa.Kim@doj.ca.gov

BEFORE THE DEPARTMENT OF JUSTICE

OFFICE OF THE ATTORNEY GENERAL

STATE OF CALIFORNIA

In the Matter of the Investigation of: **FACEBOOK, INC.**	**INVESTIGATIVE INTERROGATORIES [SET TWO]** GOV. CODE § 11180 ET SEQ.

To Benjamin A. Powell, Esq.: You are hereby served on behalf of Facebook, Inc. pursuant to your agreement to accept service on your client's behalf.

Pursuant to the powers conferred by Article 2 of Chapter 2 of Division 3 of Title 2 of the Government Code of California (Cal. Gov. Code, § 11180 et seq.) on the Attorney General, as head of the California Department of Justice, which powers and authority to conduct the above entitled investigation have been delegated to the undersigned, an officer of that Department,

FACEBOOK, INC.

IS HEREBY COMMANDED to answer separately and fully in writing, under oath, within thirty days of service hereof, each of the following interrogatories.

INSTRUCTIONS FOR COMPLIANCE

1. The RELEVANT PERIOD for these investigatory interrogatories is January 1, 2013 through December 31, 2018, unless otherwise expressly stated herein.

2. Each answer must be as complete and straightforward as the information reasonably available to Facebook, Inc. (hereafter "FACEBOOK"), including the information possessed by FACEBOOK's attorneys or agents, permits. If an interrogatory cannot be answered completely, answer it to the extent possible, specifying the reasons for FACEBOOK's inability to answer the remainder of the interrogatory and stating whatever information, knowledge, or belief that FACEBOOK has concerning the unanswered portion thereof.

3. As used herein, the past tense includes the present and future tenses, the present tense includes the past and future tenses, and the future tense includes the past and present tenses; tenses must be construed in the manner that would include, rather than exclude, information.

4. As used herein, the singular includes the plural and the plural includes the singular, and must be construed in the manner that would include, rather than exclude, information.

5. If FACEBOOK is asserting a privilege or making an objection to an interrogatory, FACEBOOK must specifically assert the privilege or state the objection in FACEBOOK's written response, and set forth in detail the basis for FACEBOOK's objection or assertion of the privilege. If an objection pertains to only a portion of an interrogatory, or a word, phrase, or clause contained in it, FACEBOOK must respond to the remainder of the Interrogatory.

6. These Investigative Interrogatories have been issued in connection with an investigation within the scope of section 131 of the California Penal Code.

7. FACEBOOK's written responses shall be delivered to the California Department of Justice, Office of the Attorney General, 1300 "I" Street, Sacramento, CA 95814-2919, ATTN: Deputy Attorney General Lisa B. Kim.

DEFINITIONS

For purposes of this set of investigatory interrogatories, the terms set forth below are defined as follows:

8. "APIs" has the same meaning used at https://developers.facebook.com/docs/apis-and-sdks/ and liked webpages, and the similar software that existed in the past.

9. "APPS OTHERS USE" means the settings used to limit data accessible to THIRD PARTY APPLICATIONS that USERS' FRIENDS installed, as set out on page 19 et seq. of the March 15, 2019 letter from Benjamin A. Powell to Stacey D. Schesser and Lisa B. Kim.

10. "AUDIENCE SELECTOR TOOL" means the setting used to set the audience for "status updates, photos and other things you share," as explained at https://www.facebook.com/help/120939471321735.

11. "DATA CONTROLS" means the settings that a USER can use to govern the sharing of USER INFORMATION with third parties, including AUDIENCE SELECTOR TOOLS, GRANULAR DATA PERMISSIONS, PLATFORM OPT-OUT, APPS OTHERS USE, and the like.

12. "DEVELOPER POLICIES" means all of the POLICIES that FACEBOOK expected DEVELOPERS to abide by, including FACEBOOK's Statement of Rights and Responsibilities, Terms of Service, Date Use Policy, Platform Policy, and /or Data Policy.

13. "DEVELOPERS" means any natural or corporate person that develops an application, game, or website, that accesses information from FACEBOOK's APIs or other software.

14. "EXTENDED API ACCESS PARTNERSHIP" means a partnership formed by agreement between FACEBOOK and a DEVELOPER that allowed access to certain

FACEBOOK APIs on terms specified within the agreement, such as FB-CA-CAAG-0002916, and beyond those terms offered to typical THIRD PARTY APPLICATIONS on the FACEBOOK Platform. This definition includes agreements performing the same general function, even if not titled as an "Extended API Addendum."

15. "EXTENDED API ACCESS PARTNER(S)" means the entity or entities with whom FACEBOOK has an EXTENDED API ACCESS PARTNERSHIP.

16. "FACEBOOK PRODUCT" means the social networking online service operated by FACEBOOK, Inc. where USERS access content, including through THIRD PARTY APPLICATIONS, websites, and games. For purposes of these interrogatories, FACEBOOK PRODUCT means content accessed online at www.facebook.com and FACEBOOK's mobile application, but does not include acquired properties, such as Instagram and WhatsApp.

17. "FRIEND" means a USER who is connected to another USER on the FACEBOOK PRODUCT.

18. "GRANULAR DATA PERMISSIONS" refers to the setting used to limit data shared with THIRD PARTY APPLICATIONS as set out at page 4 *et seq.* of the March 15, 2019 letter from Benjamin A. Powell to Stacey D. Schesser and Lisa B. Kim.

19. "INSTANT PERSONALIZATION" means the product that FACEBOOK offered that used FACEBOOK USER INFORMATION to provide tailored and integrated USER experiences on select partners' websites, as described by FACEBOOK in its December 18, 2018 Newsroom post found online at https://newsroom.fb.com/news/2018/12/facebooks-partners/.

20. "INSTANT PERSONALIZATION PARTNER(S)" means the entity or entities with whom FACEBOOK partnered for INSTANT PERSONALIZATION.

21. "INSTANT PERSONALIZATION PARTNERSHIP" means the relationship FACEBOOK had with INSTANT PERSONALIZATION PARTNERS.

22. "INTEGRATION PARTNER(S)" means the entity or entities with whom FACEBOOK has an INTEGRATION PARTNERSHIP.

23. "INTEGRATION PARTNERSHIP(S)" means the relationship FACEBOOK has with companies that built integrations for a variety of devices, operating systems, and other

products, as described by FACEBOOK in Appendix A of the July 20, 2018 letter Anjan Sahni sent to Stacey D. Schesser and Lisa B. Kim.

24. "PLATFORM OPT-OUT" means the setting used to disable the FACEBOOK platform as set out at page 10 et seq. of the March 15, 2019 letter from Benjamin A. Powell to Stacey D. Schesser and Lisa B. Kim.

25. "POLICY" or "POLICIES" mean any formal or informal policy, procedure, rule, guideline, collaborative document, directive, instruction, OR practice, whether written or unwritten, that YOU expect YOUR employees to follow in performing their jobs.

26. "PROFILE CONTROLS" means the settings that control what information in a USER's profile is shared with other USERS through AUDIENCE SELECTOR TOOLS, such as phone number, email, current city, birthday, relationship status, work, and education.

27. "SHARE" or "SHARES" or "SHARING" or "SHARED" means to provide, communicate, transfer, release, disclose, disseminate, sell, rent, trade, OR otherwise make accessible or available in writing, electronically, or by other means.

28. "THIRD PARTY APPLICATION(S)" shall have the same meaning as the terms "Platform Application(s)," "application(s)," and "app" used in FACEBOOK's policies produced to the California Attorney General bearing the Bates Labels FB-AG-00000001 through FB-CA-CAAG-00000305.

29. "USER(S)" means the individuals who maintain an account and can generally access the typical FACEBOOK experience via website or mobile application in a personal capacity.

30. "USER INFORMATION" means any information related to the FACEBOOK PRODUCT that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, the following information: name; physical address, including street name and name of a city or town; telephone number; email address; online contact information, including a screen name, username, or social network profile that functions as online contact information; user account credentials; a persistent identifier such as a user number held in a cookie or a processor serial number; a unique device identifier or a universally

unique identifier, including FBID; geolocation information, including GPS-based location information and network-based or cell-based location information; longitude and latitude data; education; employment; employment history; and any other social media content generated by OR associated with a particular individual, including status updates, likes, OR group affiliations.

31. "YOU" or "YOUR" or "FACEBOOK" means FACEBOOK, Inc. and its past or present officers, agents, employees, attorneys, predecessors, affiliates, subsidiaries, parent companies, former business names, and dbas, and anyone acting on YOUR behalf or at YOUR direction.

INTERROGATORIES

INTERROGATORY NO. 24

Provide, for each year during the RELEVANT PERIOD, the number of FACEBOOK USERS that indicated that they currently resided in California.

INTERROGATORY NO. 25

Provide, for each year during the RELEVANT PERIOD, the default settings for each of the following DATA CONTROLS:

(a) AUDIENCE SELECTOR TOOL for status updates (e.g., "Who can see your future posts?");

(b) AUDIENCE SELECTOR TOOL for birthday;

(c) AUDIENCE SELECTOR TOOL for friends list;

(d) AUDIENCE SELECTOR TOOL for email;

(e) AUDIENCE SELECTOR TOOL for who could search for and find a person's profile by contact information;

(f) GRANULAR DATA PERMISSIONS;

(g) PLATFORM OPT OUT; and,

(h) APPS OTHERS USE.

INTERROGATORY NO. 26

Provide, for each year during the RELEVANT PERIOD, the number of FACEBOOK USERS in California, expressed as a total number and percent of total USERS (or in the United States, if California data is not available), who changed their default settings for each of the following DATA CONTROLS:

(a) AUDIENCE SELECTOR TOOL for status updates (e.g., "Who can see your future posts?");

(b) AUDIENCE SELECTOR TOOL for Birthday;

(c) AUDIENCE SELECTOR TOOL for Friends List;

(d) AUDIENCE SELECTOR TOOL for email;

(e) AUDIENCE SELECTOR TOOL for who could look-up a person's profile by contact information;

(f) GRANULAR DATA PERMISSIONS;

(g) PLATFORM OPT OUT; and,

(h) APPS OTHERS USE.

INTERROGATORY NO. 27

If a USER set their PROFILE CONTROLS to "Friends," "Friends of Friends," or "Only Me," explain what, if any, non-public USER INFORMATION the following entities could access during the RELEVANT PERIOD:

(a) A THIRD PARTY APPLICATION;

(b) An experience provided by an INTEGRATION PARTNERSHIP;

(c) A website using information under an INSTANT PERSONALIZATION PARTNERSHIP;

(d) An application subject to an EXTENDED API ACCESS PARTNERSHIP; and,

(e) Any third party entity not covered in the responses to subparts (a) through (d).

INTERROGATORY NO. 28

If a USER disabled FACEBOOK'S platform for THIRD PARTY APPLICATIONS by using the PLATFORM OPT-OUT setting, explain what, if any, non-public USER INFORMATION the following entities could access during the RELEVANT PERIOD:

(a) A THIRD PARTY APPLICATION;

(b) An experience provided by an INTEGRATION PARTNERSHIP;

(c) A website using information under an INSTANT PERSONALIZATION PARTNERSHIP;

(d) An application subject to an EXTENDED API ACCESS PARTNERSHIP; and,

(e) Any third party not covered in the responses to subparts (a) through (d).

INTERROGATORY NO. 29

If a USER sets their APPS OTHERS USE settings to minimize or eliminate data being shared about a USER through FRIENDS, explain what, if any, non-public USER INFORMATION the following entities could access about a USER through FRIENDS that had installed the entity's relevant app, website, game, or experience during the RELEVANT PERIOD:

(a) A THIRD PARTY APPLICATION;

(b) An experience provided by an INTEGRATION PARTNERSHIP;

(c) A website using information under an INSTANT PERSONALIZATION PARTNERSHIP;

(d) An application subject to an EXTENDED API ACCESS PARTNERSHIP; and,

(e) Any third party not covered in the responses to subparts (a) through (d).

INTERROGATORY NO. 30

If a USER implemented FACEBOOK's DATA CONTROLS to minimize the USER INFORMATION that is SHARED with others, including setting all PROFILE CONTROLS to "Friends," disabling Platform through the PLATFORM OPT-OUT, and restricting all data sharing under the APPS OTHERS USE, describe what USER INFORMATION each of the following could access during the RELEVANT PERIOD:

(a) A THIRD PARTY APPLICATION;

(b) An experience provided by an INTEGRATION PARTNERSHIP;

(c) A website using information under an INSTANT PERSONALIZATION PARTNERSHIP;

(d) An application subject to an EXTENDED API ACCESS PARTNERSHIP; and,

(e) Any third party not covered in the responses to subparts (a) through (d).

INTERROGATORY NO. 31

Provide the following information about any DEVELOPERS that could access non-public USER INFORMATION through the USER's FRIEND, despite the USER engaging the APPS OTHERS USE control:

(a) Identity of the third party;

(b) What USER INFORMATION it could access;

(c) Whether the third party could access data through FRIENDS of FRIENDS;

(d) When the access began and ended;

(e) The reasons FACEBOOK allowed access to USER INFORMATION; and,

(f) What disclosures provided notice to USERS that their data could be shared in this way.

INTERROGATORY NO. 32

Describe the process by which FACEBOOK reviewed, developed, and approved changes to DATA CONTROLS during the RELEVANT PERIOD.

INTERROGATORY NO. 33

Identify, by name and team assignment, all the individuals at FACEBOOK who developed and approved changes to Facebook's DATA CONTROLS during the RELEVANT PERIOD.

INTERROGATORY NO. 34

Describe the review, evaluation, and testing of any new or modified DATA CONTROL during the RELEVANT PERIOD, including how FACEBOOK tested or evaluated a USER's

response or understanding of a new or modified DATA CONTROL through usability or A/B testing.

INTERROGATORY NO. 35

Describe the "coding rules" that "automatically identify and review apps that engage in acts that signal potentially abusive behavior" identified on page 11 of the July 20, 2018 letter from Anjan Sahni to Stacey D. Schesser and Lisa B. Kim.

INTERROGATORY NO. 36

State the number of times that the "coding rules" identified on page 11 of the July 20, 2018 letter from Anjan Sahni to Stacey D. Schesser and Lisa B. Kim, detected a potential abuse of FACEBOOK's DEVELOPER POLICIES during the RELEVANT PERIOD, broken down by year and for each instance explain who the DEVELOPER was and what coding rule was implicated.

INTERROGATORY NO. 37

For each year during the RELEVANT PERIOD, state the number of times that FACEBOOK received a report of a potential violation of its DEVELOPER POLICIES by a DEVELOPER from each of the following sources: (a) USERS; (b) FACEBOOK employees; (c) the press; and (d) security or white-hat researchers.

INTERROGATORY NO. 38

Explain the term "shielded app," as that term is used in the document bearing the Bates label FB-CA-CAAG-00037551.

INTERROGATORY NO. 39

Describe the manner in which YOU enforced DEVELOPER POLICIES on DEVELOPERS of "shielded apps," as that term is used in the document bearing the Bates label FB-CA-CAAG-00037551. Please identify any differences in the manner in which YOU enforced DEVELOPER POLICIES, or any other applicable POLICIES, against "shielded apps" as compared to other THIRD PARTY APPLICATIONS.

INTERROGATORY NO. 40

For each year during the RELEVANT PERIOD, specify how many enforcement actions YOU undertook in each of the following categories identified in the enforcement rubric set forth in the document bearing the Bates label FB-CA-CAAG-00019954:

(a) Surface or escalate to point of contact;

(b) Warning (of any length);

(c) Moratorium;

(d) Removal from approved advertiser list;

(e) Disable credits;

(f) Disable; and,

(g) Escalate to Legal for a cease and desist letter.

INTERROGATORY NO. 41

Identify all instances when FACEBOOK deviated its response from the "recommended action" for each perceived violation of DEVELOPER POLICIES, as set forth in the document bearing the Bates label FB-CA-CAAG-00019954. For each instance, state the action taken, and the reason why FACEBOOK deviated its response.

INTERROGATORY NO. 42

Describe what steps FACEBOOK took, if any, to ensure that applications created pursuant to an INTEGRATED PARTNERSHIP or an EXTENDED API ACCESS PARTNERSHIP did not access or use data for any purpose other than what was authorized by FACEBOOK's agreements with the partner.

INTERROGATORY NO. 43

For each year during 2013 to 2017, state how many times FACEBOOK has suspended or disabled access to USER INFORMATION by THIRD PARTY APPLICATIONS, or their DEVELOPERS, for violation of the following DEVELOPER POLICIES requirements:

Developers shall: only request the data needed to operate their application; only use the data received from Facebook for their application; obtain explicit consent

from the user who provided the data to Facebook before using it for any purpose other than displaying it back to the user;

Developers shall not: transfer any data that they receive from Facebook; sell user data; use Facebook user IDs for any purpose outside of their applications; use a user's friend list outside of their application; access a user's friend list when a friend connects with that app; if a friend grants specific permission, use that content and information other than in connection with that friend.

INTERROGATORY NO. 44

Has FACEBOOK ever suspended or disabled access to USER INFORMATION by an INTEGRATED PARTNER, EXTENDED API ACCESS PARTNER, or INSTANT PERSONALIZATION PARTNER because the DEVELOPER appeared to have violated either FACEBOOK's DEVELOPER POLICIES regarding USER INFORMATION or the parties' agreement regarding USER INFORMATION? If so, please identify the DEVELOPER, the details of the suspected violation, and how FACEBOOK learned of the suspected violation.

INTERROGATORY NO. 45

Excluding 1) USERS, 2) INTEGRATED PARTNERS, 3) INSTANT PERSONALIZATION PARTNERS, and 4) THIRD PARTY APPLICATION DEVELOPERS operating under FACEBOOK's DEVELOPER POLICIES, identify any other persons or entities to whom FACEBOOK granted access to USER INFORMATION, by:

(a) The name of the third party;

(b) The USER INFORMATION available to the third party;

(c) The reason the third party was granted access; and,

(d) The dates that access began and ended.

INTERROGATORY NO. 46

Describe the different FACEBOOK APIs that DEVELOPERS could use to access USER INFORMATION during the RELEVANT PERIOD.

INTERROGATORY NO. 47

Identify the APIs that each of the following entities could use to access USER INFORMATION during the RELEVANT PERIOD:

(a) A DEVELOPER of a THIRD PARTY APPLICATION;

(b) An INTEGRATION PARTNER;

(c) An INSTANT PERSONALIZATION PARTNER; and,

(d) An EXTENDED API ACCESS PARTNER.

INTERROGATORY NO. 48

Did FACEBOOK ever factor a DEVELOPER's advertising purchase history or amount spent into the decision to enter into, continue, or terminate an EXTENDED API ACCESS PARTNERSHIP? If so, please describe the circumstances.

INTERROGATORY NO. 49

Did FACEBOOK ever factor a DEVELOPER's advertising purchase history or amount spent into the decisions as to what capabilities or access to USER INFORMATION to grant pursuant to an EXTENDED API ACCESS PARTNERSHIP? If so, please describe the circumstances.

INTERROGATORY NO. 50

Describe FACEBOOK's history of auditing the use or handling of USER INFORMATION by DEVELOPERS, including whether FACEBOOK ever considered conducting audits, actually conducted any audits, and, if so, what it found. Please exclude: (A) information regarding an

///

///

///

///

///

///

///

///

individual investigation into a particular DEVELOPER'S use of data, and (B) information about the ADI process previously disclosed by FACEBOOK.

FAILURE TO COMPLY WITH THIS SUBPOENA WILL SUBJECT YOU TO THE PROCEEDINGS AND PENALTIES PROVIDED BY LAW.

Dated: June 17, 2019

XAVIER BECERRA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER
Supervising Deputy Attorney General
LISA B. KIM
SUSAN SAYLOR
MICAH C.E. OSGOOD
MANEESH SHARMA
Deputy Attorneys General

LISA B. KIM
Deputy Attorney General

DECLARATION OF SERVICE BY E-MAIL

Matter Name: In the Matter of the Investigation of: FACEBOOK, INC.

I declare:

I am employed in the Office of the Attorney General, which is the office of a member of the California State Bar, at which member's direction this service is made. I am 18 years of age or older and not a party to this matter; my business address is 300 South Spring Street, Suite 1702, Los Angeles, CA 90013.

On June 17, 2019, I served the attached **INVESTIGATIVE INTERROGATORIES [SET TWO]** by placing a true copy thereof enclosed in a sealed envelope with postage thereon fully prepaid, in the United States Mail at Los Angeles, California, addressed as follows:

Benjamin A. Powell
Maury Riggan
WilmerHale
1875 Pennsylvania Avenue NW
Washington, DC 20006
Benjamin.Powell@wilmerhale.com
Maury.Riggan@wilmerhale.com

I declare under penalty of perjury under the laws of the State of California the foregoing is true and correct and that this declaration was executed on June 17, 2019, at Los Angeles, California.

Carol Chow
Declarant

Signature

SF2018400570
53504613.docx

CM-010

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address):
Micah C.E. Osgood (SBN 255239)
Office of the Attorney General
455 Golden Gate Ave. Suite 11000
San Francisco, CA 94102
TELEPHONE NO.: (415) 510-4400 FAX NO.:
ATTORNEY FOR (Name): People of the State of California, Petitioner

FOR COURT USE ONLY

FILED
San Francisco County Superior Court
NOV 06 2019
CLERK OF THE COURT
By: ANGELICA SUNGA Deputy Clerk

SUPERIOR COURT OF CALIFORNIA, COUNTY OF San Francisco
STREET ADDRESS: 400 McAllister Avenue
MAILING ADDRESS:
CITY AND ZIP CODE: San Francisco, CA 94102
BRANCH NAME: Civic Center Courthouse

CASE NAME:
People of the State of California v. Facebook, Inc.

CASE NUMBER: CGC-19-516916

JUDGE:

DEPT:

CIVIL CASE COVER SHEET

☑ **Unlimited** (Amount demanded exceeds $25,000) ☐ **Limited** (Amount demanded is $25,000 or less)

Complex Case Designation

☐ **Counter** ☐ **Joinder**

Filed with first appearance by defendant (Cal. Rules of Court, rule 3.402)

Items 1–6 below must be completed (see instructions on page 2).

1. Check **one** box below for the case type that best describes this case:

Auto Tort
- ☐ Auto (22)
- ☐ Uninsured motorist (46)

Other PI/PD/WD (Personal Injury/Property Damage/Wrongful Death) Tort
- ☐ Asbestos (04)
- ☐ Product liability (24)
- ☐ Medical malpractice (45)
- ☐ Other PI/PD/WD (23)

Non-PI/PD/WD (Other) Tort
- ☐ Business tort/unfair business practice (07)
- ☐ Civil rights (08)
- ☐ Defamation (13)
- ☐ Fraud (16)
- ☐ Intellectual property (19)
- ☐ Professional negligence (25)
- ☐ Other non-PI/PD/WD tort (35)

Employment
- ☐ Wrongful termination (36)
- ☐ Other employment (15)

Contract
- ☐ Breach of contract/warranty (06)
- ☐ Rule 3.740 collections (09)
- ☐ Other collections (09)
- ☐ Insurance coverage (18)
- ☐ Other contract (37)

Real Property
- ☐ Eminent domain/Inverse condemnation (14)
- ☐ Wrongful eviction (33)
- ☐ Other real property (26)

Unlawful Detainer
- ☐ Commercial (31)
- ☐ Residential (32)
- ☐ Drugs (38)

Judicial Review
- ☐ Asset forfeiture (05)
- ☐ Petition re: arbitration award (11)
- ☐ Writ of mandate (02)
- ☐ Other judicial review (39)

Provisionally Complex Civil Litigation (Cal. Rules of Court, rules 3.400–3.403)
- ☐ Antitrust/Trade regulation (03)
- ☐ Construction defect (10)
- ☐ Mass tort (40)
- ☐ Securities litigation (28)
- ☐ Environmental/Toxic tort (30)
- ☐ Insurance coverage claims arising from the above listed provisionally complex case types (41)

Enforcement of Judgment
- ☐ Enforcement of judgment (20)

Miscellaneous Civil Complaint
- ☐ RICO (27)
- ☐ Other complaint *(not specified above)* (42)

Miscellaneous Civil Petition
- ☐ Partnership and corporate governance (21)
- ☑ Other petition *(not specified above)* (43)

2. This case ☐ is ☑ is not complex under rule 3.400 of the California Rules of Court. If the case is complex, mark the factors requiring exceptional judicial management:
   a. ☐ Large number of separately represented parties
   b. ☐ Extensive motion practice raising difficult or novel issues that will be time-consuming to resolve
   c. ☐ Substantial amount of documentary evidence
   d. ☐ Large number of witnesses
   e. ☐ Coordination with related actions pending in one or more courts in other counties, states, or countries, or in a federal court
   f. ☐ Substantial postjudgment judicial supervision
3. Remedies sought *(check all that apply)*: a. ☐ monetary b. ☒ nonmonetary; declaratory or injunctive relief c. ☐ punitive
4. Number of causes of action *(specify)*: N/A
5. This case ☐ is ☒ is not a class action suit.
6. If there are any known related cases, file and serve a notice of related case. *(You may use form CM-015.)*

Date: Nov. 4, 2019
Micah C.E. Osgood
(TYPE OR PRINT NAME)

(SIGNATURE OF PARTY OR ATTORNEY FOR PARTY)

NOTICE
- Plaintiff must file this cover sheet with the first paper filed in the action or proceeding (except small claims cases or cases filed under the Probate Code, Family Code, or Welfare and Institutions Code). (Cal. Rules of Court, rule 3.220.) Failure to file may result in sanctions.
- File this cover sheet in addition to any cover sheet required by local court rule.
- If this case is complex under rule 3.400 et seq. of the California Rules of Court, you must serve a copy of this cover sheet on **all** other parties to the action or proceeding.
- Unless this is a collections case under rule 3.740 or a complex case, this cover sheet will be used for statistical purposes only.

Form Adopted for Mandatory Use
Judicial Council of California
CM-010 [Rev. July 1, 2007]

CIVIL CASE COVER SHEET

Cal. Rules of Court, rules 2.30, 3.220, 3.400–3.403, 3.740;
Cal. Standards of Judicial Administration, std. 3.10
www.courtinfo.ca.gov