Attorney General of Missouri

Joshua D. Hawley **Attorney General**	Jefferson City 65102	**P.O. Box 899** **(573) 751-3321**

IN THE MATTER OF: *Via Hand Delivery*

Facebook, Inc. CID No. 34-18
April 2, 2018

CIVIL INVESTIGATIVE DEMAND

TO: Facebook, Inc.
1 Hacker Way
Menlo Park, California 94025

The Attorney General of the State of Missouri believes it to be in the public interest that an investigation be made to ascertain whether Facebook, Inc. ("Subject") has engaged in or is engaging in any practices declared to be unlawful by § 407.020, RSMo. This investigation will inquire into the representations, acts, and practices of Subject in connection with the disclosure, collection, use, retention, storing, sharing, sale, and dissemination of information and data relating to Facebook Users. The Attorney General has reason to believe that Subject's conduct in the aforementioned areas and others involves deception, fraud, false promise, misrepresentation, unfair practices, and/or the concealment, suppression, or omission of material facts within the scope of the Missouri Merchandising Practices Act.

Please note that materials and information produced pursuant to this civil investigative demand may be disclosed to other state and/or federal law-enforcement agencies pursuant to § 407.060.1, RSMo.

The Attorney General believes that You have information, documentary material, and/or physical evidence relevant to the investigation described above.

DEFINITIONS

In this Civil Investigative Demand, the following terms shall have the meanings set forth herein:

1. "You" and "Your" mean Facebook, Inc.; Facebook, Inc.'s subsidiaries, parent companies, and sister companies; and all agents, representatives, employees, independent

contractors, attorneys, and other persons acting or purporting to act on behalf of Facebook, Inc. and/or its subsidiaries, parent companies, or sister companies. This definition of "You" and "Your" applies regardless of whether the words "you" or "your" are capitalized.

2. "Document" includes every "writing," "recording," and "photograph" as Federal Rule of Evidence 1001 defines those terms, as well as any "duplicate" of any writing, recording, or photograph. "Document" includes but is not limited to electronic documents, files, databases, and records, including but not limited to emails, voicemails, text messages, calendar appointments, instant messages, MMS messages, SMS messages, iMessages, computer files, spreadsheets, and metadata. The term Document includes every draft of any other material that falls within the definition of Document.

3. "Communication" means any expression, statement, conveyance, or dissemination of any words, thoughts, statements, ideas, or information, regardless of form, format, or kind. "Communication" includes but is not limited to oral or written communications of any kind, such as telephone conversations, discussions, meetings, notes, letters, agreements, emails or other electronic communications, facsimiles, and other forms of written or oral exchange that are recorded in any way, including video recordings, audio recordings, written notes, or otherwise. Any Communication that also falls within the definition of "Document" shall constitute both a Document and a Communication for purposes of this civil investigative demand.

4. With regard to a person, "Identify" means to state with specificity the person's legal name, aliases, last-known home address, last-know business address, current employer, current job title, all known telephone numbers, and all known email addresses.

5. With regard to a Communication, "Identify" means to state with specificity the date of the Communication; the medium of communication; the location of the Communication; the name(s) and alias(es) of the person(s) who made the Communication; and the name(s) and alias(es) of all persons who were present when the statement was made, who received the Communication, who heard the Communication, or who came to know of the content of the Communication at a later time.

6. "All" and "any" shall each be construed to encompass the meanings of the words "all" and "any."

7. "Person" means any natural person, corporation, proprietorship, partnership, association, firm, or entity of any kind.

8. "Facebook User" means any Person from or about whom Facebook has obtained any information or data, for the purpose of or in the course of providing any Facebook product or service.

9. "Facebook User Information" means information from or about an individual Facebook User.

10. "Privacy Setting" shall include any control or setting provided by You that allows a Facebook User to restrict the Persons that can access, view, collect, receive, or use their Facebook User Information.

11. "Third Party" means any Person that accesses, views, collects, receives, or uses another Person's Facebook User Information other than: (1) Facebook, Inc.; (2) a service provider of Facebook, Inc. that (i) uses the Facebook User Information for and at the direction of Facebook, Inc. and no other individual or entity and for no other purpose; and (ii) does not disclose the Facebook User Information or any individually identifiable information derived therefrom except for, and at the direction of, Facebook, Inc., for the purpose of providing services requested by a User and for no other purpose; or (3) any entity that uses the Facebook User Information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce Facebook, Inc.'s terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities. The term "Third Party" includes any application operated, owned, or controlled by any Person who constitutes a "Third Party."

12. "FTC Consent Order" means the Decision and Order issued on or about July 27, 2012 by the Federal Trade Commission in *In the Matter of Facebook, Inc.*, Docket No. C-4365, File No. 0923184.

13. "SCL" means SCL Group Limited (a/k/a Strategic Communications Laboratories); its subsidiaries, parent companies, and sister companies; and all agents, representatives, employees, independent contractors, attorneys, and other persons acting or purporting to act on behalf of SCL Group Limited and/or its subsidiaries, parent companies, or sister companies.

14. "Cambridge Analytica" means Cambridge Analytica LLC; its subsidiaries, parent companies, and sister companies; and all agents, representatives, employees, independent contractors, attorneys, and other persons acting or purporting to act on behalf of Cambridge Analytica LLC and/or its subsidiaries, parent companies, or sister companies.

15. "GSR" means Global Science Research; its subsidiaries, parent companies, and sister companies; and all agents, representatives, employees, independent contractors, attorneys, and other persons acting or purporting to act on behalf of Global Science Research and/or its subsidiaries, parent companies, or sister companies.

16. "Data Breach Incident" means the unauthorized disclosure, collection, use, retention, storing, sharing, sale, and/or dissemination of Facebook User Data to or by SCL and/or Cambridge Analytica.

DEMAND FOR DOCUMENTS AND INFORMATION

Pursuant to § 407.040, RSMo, the Attorney General demands that—no later than 10:00 a.m. (Central) on May 29, 2018—You produce the following documents and information, to the extent that they are within Your possession, custody, and/or control.

Your document production must comply with the Missouri Office of the Attorney General Production Specifications and Data Delivery Standards, a copy of which is attached hereto.

In responding to each Request contained in this civil investigative demand, You should identify—by Bates range, or by file names and locations—which Documents are responsive to each Request.

If You withhold any responsive materials based on an assertion of privilege and/or the work-product doctrine, You must produce a privilege log that provides—for each Document or Communication withheld—sufficient information to permit the Attorney General's Office to assess the applicability of the privilege and/or the work-product doctrine.

1. Produce all privacy policies for all Facebook applications, products, and platforms—including all versions of those privacy policies—that were in effect at any time from January 1, 2012 to the present, and with respect to each such policy or version, state when the policy or version was adopted.

2. Produce all privacy statements and other Documents disseminated at any time from January 1, 2012 to the present containing any representations by You to Facebook Users concerning the collection, protection, use, retention, storing, disclosure, sharing, sale, dissemination, and/or privacy of Facebook User Information.

3. Identify all categories and/or types of Facebook User Information that You have collected from or about Facebook Users from January 1, 2012 to the present, and when You began collecting each such category and/or type of information.

4. Identify the categories and/or types of Facebook User Information that constitute "personally identifiable information" within the meaning of Your privacy policy or policies.

5. Describe the Privacy Settings available to Facebook Users, from January 1, 2012 to the present, including:

a. Privacy Settings available for restricting access to or use of entire categories of Facebook User Information, the identity of each category, the ways in which Users could restrict information in each category, and the types of Facebook User Information falling within each category;

b. Privacy Settings available for restricting access to or use of specific items of Facebook User Information, the identity of each item of Facebook User Information that could be individually restricted, and the ways in which Users could restrict that item of Facebook User Information; and

c. The identity of Facebook User Information for which You did not provide any Privacy Settings.

To the extent that the Privacy Settings provided by You to Facebook Users changed at any time from January 1, 2012 to the present, describe in detail the nature of such changes and the date such changes were effective.

6. Describe every way in which You provide or make available any Facebook User Information to any Third Party.

7. Describe the conditions, terms, and stipulations under which Facebook provides Facebook User Information to Third Parties.

8. Produce all guidelines, procedures, manuals, and terms of service related to the disclosure of Facebook User Information to Third Parties.

9. Describe the general conditions, terms, or stipulations, placed upon Third Parties' use or disclosure of Facebook User Information.

10. Produce all guidelines, procedures, manuals, and terms of service related to Third Parties' use or disclosure of Facebook User Information.

11. Describe how Facebook monitored or tracked the Facebook User Information that Third Parties obtained and/or used.

12. Describe how Facebook ensured that Third Parties did not have access to more or different Facebook User Information than was authorized.

13. Describe all security protocols, alerts, and flags that Facebook employed that would indicate to Facebook that a Third Party had obtained more or different Facebook User Information than was authorized.

14. Describe all guidelines, policies, procedures, manuals, and protocols prescribing the measures Facebook took to ensure that Facebook User Information acquired by any Third Party would not be used for unauthorized purposes.

15. Describe all audits, controls, or other measures Facebook undertook to verify how Third Parties use Facebook User Information.

16. Describe all guidelines, policies, procedures, manuals, and protocols prescribing what, if anything, Facebook would do upon discovering that a Third Party had obtained more or different Facebook User Information than was authorized.

17. Describe all guidelines, policies, procedures, manuals, and protocols setting forth what, if anything, Facebook would do to ensure that Facebook User Information that had been accessed by an unauthorized person or persons was deleted.

18. Produce all Documents identified in, referenced in, relied upon in answering, or relating to Requests 11-17 above.

19. Produce each written privacy program that You established, implemented, and/or maintained as required by Section IV of the FTC Consent Order.

20. Produce each privacy assessment and/or report obtained by You as required by Section V of the FTC Consent Order.

21. For each privacy assessment and/or report produced in response to Request 20, produce all Documents and Communications relied upon to prepare the assessment or report.

22. Produce all documents prepared by or on behalf of You that contradict, qualify, or call into question Your compliance with the FTC Consent Order.

23. Produce each report that You submitted to the FTC setting forth the manner and form of Your purported compliance with the FTC Consent Order as required by Section IX of the FTC Consent Order.

24. State the date on which the Facebook platform application "thisisyourdigitallife" was launched and the date on which it was terminated.

25. Identify all other Facebook platform applications developed, owned, or associated with Aleksandr Kogan, SCL, Cambridge Analytica, and/or GSR, including the dates such applications were launched and/or terminated.

26. Describe in detail Your efforts to identify any other Facebook platform applications developed, owned, or associated with Aleksandr Kogan, SCL, Cambridge Analytica, and/or GSR.

27. Provide a complete description of the specific categories and/or types of Facebook User Information that the application "thisisyourdigitallife" was able to view, collect, use, retain, and/or store regarding Facebook Users that installed the application. If these categories and/or types of Facebook User Information changed over time, describe these changes in detail and provide the date(s) of such changes.

28. Provide a complete description of the specific categories and/or types of Facebook User Information that the application "thisisyourdigitallife" was able to view, collect, use, retain, and/or store regarding Facebook Users that had not installed the application. If these categories and/or types of Facebook User Information changed over time, describe these changes in detail and provide the date(s) of such changes.

29. Provide a timeline that describes in detail the facts and circumstances surrounding how You learned that Facebook User Information collected, used, retained, and/or stored by "thisisyourdigitallife" had been or may have been shared, sold, and/or disseminated to unauthorized Third Parties including, but not limited to, SCL and/or Cambridge Analytica, including:

a. the specific date when You first learned of a potential unauthorized disclosure;

b. how You learned of the potential unauthorized disclosure; and

c. when and how Facebook executive officers were made aware of the potential unauthorized disclosure, and the identity of those executive officers.

30. Describe in detail Your efforts to investigate and/or mitigate the Data Breach Incident, including the dates of inception, the names of all outside firms or contractors utilized in this investigation, and the findings and conclusions of these investigations.

31. Provide a timeline that describes in detail the Facebook User Information collected, used, retained, and/or stored by "thisisyourdigitallife" that was or is believed to have been shared, sold, and/or disseminated to unauthorized Third Parties including, but not limited to, SCL and/or Cambridge Analytica, including:

a. the specific categories and/or types of Facebook User Information that was or is believed to have been shared; and

b. the number of instances and date(s) when such Facebook User Information was or is believed to have been shared.

32. Describe when and how You learned that thisisyourdigitallife obtained Facebook User Information for friends of Facebook Users who installed the thisisyourdigitallife application.

33. Describe the efforts taken by Facebook or a Third Party on its behalf to determine or confirm the extent of personal information accessed and downloaded by thisisyourdigitallife.

34. Describe in detail all plans, policies, steps and/or procedures that Facebook currently has in place, or is developing, to prevent future data breach incidents and the timeline for implementing such plans, policies, steps, or procedures.

35. Describe all measures that You have taken to protect the individuals affected by this Data Breach Incident.

36. Describe how You ensured that Aleksandr Kogan, Christopher Wylie, SCL, Cambridge Analytica, and/or GSR had deleted Facebook User Information they were not authorized to have.

37. Produce all contracts and agreements between You and any of the following:

a. Aleksandr Kogan;

b. Christopher Wylie;

c. SCL;

d. Cambridge Analytica; or

e. GSR.

38. Produce all contracts and agreements in Your possession, custody, or control to which any of the following is a party:

a. Aleksandr Kogan;

b. Christopher Wylie;

c. SCL;

d. Cambridge Analytica; or

e. GSR.

39. Produce all Documents and Communications between You and any of the following:

a. Aleksandr Kogan;

b. Christopher Wylie;

c. SCL;

d. Cambridge Analytica; or

e. GSR.

40. Produce Documents sufficient to identify when Facebook contracted with a Third Party forensic agency to ensure that Christopher Wylie and/or Cambridge Analytica had deleted the Facebook User Information that they were not authorized to have.

41. Produce all Documents concerning internal or Third Party investigative reports or audits, including forensic reports, performed by or for Facebook concerning the Data Breach Incident.

42. Produce all Documents concerning Facebook's investigation(s) of the Data Breach Incident, including the findings and conclusions of those investigations.

43. Produce all Documents concerning any internal Facebook Communications concerning the Data Breach Incident, including Documents sufficient to identify when the first Data Breach Incident-related Communications were made to any member of the executive staff.

44. State the number of Facebook Users in the United States, and the number of Missouri Facebook users, that installed the Facebook platform application "thisisyourdigitallife."

45. State the number of Facebook Users in the United States, and the number of Missouri Facebook users, whose Facebook User Information was disclosed, collected, used, retained, stored, shared, sold, or disseminated to SCL and/or Cambridge Analytica.

46. With respect to Missouri Facebook Users whose Facebook User Information was or may have been viewed, disclosed, collected, used, retained, stored, shared, sold, and/or disseminated to SCL and/or Cambridge Analytica, state whether any such Facebook User Information included or disclosed:

a. a Missouri Facebook User's Social Security number;

b. a Missouri Facebook User's driver's license number or other unique identification number created or collected by a government body;

c. a Missouri Facebook User's financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;

d. a Missouri Facebook User's unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

e. information regarding a Missouri Facebook User's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

f. information regarding a Missouri Facebook User's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual.

47. State whether You have provided notice of the Data Breach Incident to Missouri Facebook Users whose Facebook User Information was or may have been viewed, disclosed, collected, used, retained, stored, shared, sold, and/or disseminated to SCL and/or Cambridge Analytica.

If You have sent such notice:

a. state the dates(s) that You sent the notice(s);

b. describe the manner in which the notice(s) was/were provided;

c. produce an exemplar of the notice(s);

d. state the number of notices sent to such Missouri Facebook Users; and

e. if You have not sent such notice, state the reason(s) for failing to provide such notice.

48. Describe in detail the delay between Your discovery of the Data Breach Incident and Your public announcement of the Data Breach Incident, including the identity of Your officers and employees involved in any decision to delay publicly announcing the Data Breach Incident.

49. Produce all Documents identified in, referred to in, used in preparation of, or relating to any of Your responses to any Request above.

50. Describe in detail all Facebook User Information collected or obtained by Facebook's application for use on Android devices.

51. Produce all privacy policies and other forms of notice that You contend provided notice to Facebook Users of the Facebook User Information that would be collected or obtained by Facebook's application for us on Android devices.

52. Produce all Communications between You, on the one hand, and Google, Inc. or Google, LLC—including all employees, officers, and agents of Google, Inc. and/or Google, LLC—on the other hand, relating to the collection or obtaining of Facebook User Information by Facebook's application for use on Android devices.

53. Identify every political campaign and every political action committee with whom Facebook has shared any Facebook User Information. For each political campaign and political action committee identified, describe in detail the Facebook User Information shared with the campaign or committee, the date(s) on which Facebook shared the Facebook User Information; any compensation that Facebook received for sharing that Facebook User Information, whether Facebook Users were notified that Facebook intended to or had shared that Facebook User Information, and the provisions of all applicable privacy policies (if any) that You contend authorized such information sharing.

54. For each political campaign and political action committee identified in response to Request 53, produce all Communications between Facebook and the campaign or committee.

55. For each political campaign and political action committee identified in response to Request 53, produce all contracts between Facebook and the campaign or committee.

56. For each political campaign and political action committee identified in response to Request 53, produce all notices provided to Facebook Users that Facebook intended to or had shared Facebook User Information with the campaign or committee.

57. Produce all other Documents reflecting or relating to the sharing of any Facebook User Information with any political campaign or political action committee.

58. Produce all Communications between You and Carol Davidsen.

59. Produce all Communications between You and any employee, volunteer, independent contractor, or agent of the campaign Obama for America relating to the sharing of Facebook User Information.

60. Produce all Documents and calendar entries reflecting any meeting or telephone call involving any employee, volunteer, independent contractor, or agent of the campaign Obama for America relating to the sharing of Facebook User Information.

The Attorney General's Office may serve additional or subsequent civil investigative demands on You.

Please note that pursuant to § 407.080, RSMo, certain acts done with the intent to avoid, evade, or prevent compliance in whole or in part with any civil investigative constitute a Class A misdemeanor, which is punishable by a fine not to exceed $1,000 for individuals and $5,000 for corporations, or by imprisonment for a term of not more than one year, or both a fine and imprisonment.

No extension of the deadline for compliance with this civil investigative demand shall be effective unless it is reflected in a writing executed by an authorized representative of the Attorney General.

Submit the following Certification of Compliance and all responsive documents and information to:

Michael Martinich-Sauter
Missouri Attorney General's Office
P.O. Box 899
Jefferson City, Missouri 65102
Michael.martinich-sauter@ago.mo.gov

Michael Martinich-Sauter, Mo. Bar No. 66065
Missouri Attorney General's Office
Supreme Court Building
207 W. High Street
P.O. Box 899
Jefferson City, Missouri 65102
(573) 751-8145
michael.martinich-sauter@ago.mo.gov

Joseph Schlotzhauer, Mo. Bar No. 63128
Missouri Attorney General's Office

Michael A.T. Schwalbert, Mo. Bar No. 63229
Missouri Attorney General's Office

In the Matter of:

Facebook, Inc. CID NO. 34-18

CERTIFICATION OF COMPLIANCE

I/We hereby certify that all documents and information required by Civil Investigative Demand No. 34-18 which is in the possession, custody, control, or knowledge of, ______ ____has been submitted to the Missouri Attorney General as directed herein.

Signature ________________________

Title ____________________________

Sworn to before me this ___ day of __________, 20___.

____

Notary Public

My Commission Expires:

IN THE STATE OF ________________)

) SS

COUNTY OF ____________________)

AFFIDAVIT

Before me, the undersigned authority, personally appeared, __________________ who, being by me duly sworn, deposed as follows:

My name is _________________________________, I am of sound mind, capable of making this affidavit, and personally acquainted with the facts herein stated:

I am the custodian of the records of ________________________________.

Attached hereto are ______ pages of records from __________________________.

These ______ pages of records are kept by ________________________________ in the regular course of business, and it was the regular course of business of _______________ for an employee or representative of __________________________ with knowledge of the act, event, condition, opinion, or diagnosis recorded to make the record or to transmit information thereof to be included in such record; and the record was made at or near the time of the act, event, condition, opinion or diagnosis. The records attached hereto are the original or exact duplicates of the original.

Affiant

In witness whereof, I have hereunto subscribed my name and affixed my official seal this ____ day of ________________, 20___.

[SEAL] Notary Public

My Commission Expires: ___________

Missouri Office of the Attorney General Production Specifications and Data Delivery Standards

A. Document Categories

1. Email, Attachments, and Other Electronic Messages

Email and other electronic messages (e.g., instant messages (IMs)) should be produced either natively or as image files with related searchable text, metadata and bibliographic information. Depending on how the company's systems represent names in email messages or IMs, we may require a table of names or contact lists from custodians.

Email repositories, also known as email databases (e.g., Outlook .PST, Lotus .NSF), can contain a variety of items, including messages, calendars, contacts, tasks, etc. For purposes of production, responsive items should include the "Email" metadata/database fields below, including but not limited to all parent items (mail, calendar, contacts, tasks, notes, etc.) and child files (attachments of files to email or other items), with the parent/child relationship preserved. Similar items found and collected outside an email repository (e.g., .MSG, .EML, .HTM, .MHT) should be produced in the same manner.

Each IM conversation should be produced as one document.

2. **Attachments:** The parent-child relationship must be maintained with any production and notated through the load file fields provided with the production.

3. **Electronic (Loose) Documents:** Electronic documents, including, but not limited to, word-processing documents, spreadsheets, presentations, and all other electronic documents not specifically discussed elsewhere should be produced either natively or as image files with related searchable text, metadata, and bibliographic information. All passwords and encryption must be removed from electronic documents prior to production. However:

   a. **Spreadsheets:** Must be produced in native format with searchable text for the entire document, metadata, and bibliographic information. Provide only a single image of the first page of the spreadsheet or provide a single placeholder image. The placeholder image must contain at a minimum the PRODBEG and FILENAME. The Bates range for a native spreadsheet should be a single number. The linked native file name should match the PRODBEG with the appropriate file extension.

   b. **Presentations:** Must be produced in full slide image format along with speaker notes (which should follow the full images of the slides) with related searchable text, metadata, and bibliographic information. Presentations may be produced as image files with related searchable text, metadata and bibliographic information. However, the AGO retains the right to request that any presentation be produced subsequently in native format. Additionally, the AGO retains the right to request that any presentation produced in black and white be produced in color.

   c. **Hidden Text:** All hidden text (e.g., track changes, hidden columns, hidden slides, mark-ups, notes) shall be expanded and rendered in the extracted text file. For files that cannot be expanded linked native files shall be produced with the image files.

d. **Embedded Files:** All embedded objects (e.g., graphical files, Word documents, Excel spreadsheets, .wav files) that are found within a file shall be produced so as to maintain the integrity of the source document as a single document. For purposes of production the embedded files shall remain embedded as part of the original source document. Hyperlinked files must be produced as separate, attached documents. Any objects that cannot be rendered to images and extracted text must be produced as separate extracted files treated as attachments to the original file.

e. **Image-Only Files:** All image-only files (non-searchable .PDFs, multi-page TIFFs, Snipping Tool screenshots, etc., as well as all other images that contain text) shall be produced with associated OCR text, metadata, and bibliographic information.

f. **Archive File Types Archive file types** (e.g., .zip, .rar): Must be uncompressed for processing. Each file contained within an archive file should be produced as a child to the parent archive file. If the archive file is itself an attachment, that parent/child relationship must also be preserved.

4. **Hard-Copy (or Paper) Documents**

Hard-copy documents are to be produced as black-and-white image files, except where otherwise noted with related searchable OCR text and bibliographic information. Special attention should be paid to ensure that hard-copy documents are produced as they are kept in the ordinary course, reflecting attachment relationships between documents and information about the file folders within which each document is found. In addition, multi-page documents must be produced as single documents (i.e., properly unitized) and not as several single-page documents. Where color is required to interpret the document, such as hard copy photos, and certain charts, that image must be produced in color. These color images are to be produced as .jpg format. Hard-copy photographs should be produced as color .jpg, if originally in color, or grayscale .tif files if originally in black-and-white. If documents originally in color are produced in black-and-white, the AGO retains the right to request that such documents be produced in color.

5. **Shared Resources**

Shared Resources should be produced as separate custodians if responsive custodians have access to them or if they contain responsive documents. The name of the group having access would be used as the custodian name. A list of the other custodians with access to the shared resource should be provided in the CUSTODIAN field.

6. **Other Sources:** The following types of data/document productions should be discussed with the AGO prior to any production to determine the most appropriate production format.

a. Proprietary File Types and Non-PC or Non-Windows Based Systems
b. Database(s) and/or dynamic data
c. Audio and/or video data
d. Foreign-Language data or documents

B. **De-duplication**: De-duplication, both horizontally and vertically, within and across custodians is highly encouraged for electronic documents based on the files' MD5 or SHA-1 hash values. De-duplication must be done in a way that preserves (and produces) information on blind copy (bcc) recipients of emails and other custodians whose files contain the duplicates that will be eliminated from the production.

Note: When de-duplicating horizontally (i.e. across custodians), the CUSTODIAN field must reflect all custodians that held the duplicate record(s), which would have been produced but not for the de-duplication.

C. **Email threading**

A producing party may produce the "most inclusive email threads" based on the following:

1. A "most inclusive email thread" is one that contains all of the prior or lesser-included emails, including attachments, for that branch of the e-mail thread. In an email thread, only the final-in-time document need be produced, assuming that all previous emails in the thread are contained within the final message and provided that the software used to identify these "most inclusive email threads" is able to identify any substantive differences to the thread such as changes in recipients (*e.g.*, side threads, subject line changes), selective deletion of previous thread content by sender, etc.

2. Where a prior email contains an attachment, that email and attachment shall not be removed as a "most inclusive email thread." When an email thread branches, each branch shall be treated a separate email, and should be produced separately. Each branch that is the "most inclusive email thread" may likewise be treated as the most inclusive thread of all prior or lesser included emails within that branch and only the final-in-time email for that thread need be produced.

3. The AGO retains the right to request the individual emails contained in the most inclusive email threads be produced as needed.

D. **Document Numbering**

Documents must be uniquely and sequentially Bates-numbered across the entire production, with an endorsement burned into each image. Each Bates number shall be of a consistent length, include leading zeros in the number, and unique for each produced page. Bates numbers should contain no other special characters other than hyphens (-).

E. **Privilege Designations**

Documents redacted pursuant to any claim of privilege should be designated "Redacted" in the PROPERTIES field. Appropriately redacted searchable text (OCR of the redacted images is acceptable), metadata, and bibliographic information must also be provided. All documents that are part of a document family that includes a document withheld pursuant to any claim of privilege will be designated "Family Member of Privileged Doc" in the PROPERTIES field as described in the Metadata Fields table for all other documents in its family. Placeholder images with PRODBEG, FILENAME and reason withheld (e.g., "Privileged") should be provided in place of the document images of the privileged document

F. **Load File Set/Volume Configuration**

Each production must have a unique PHYSICALMEDIA name associated with it. This PHYSICALMEDIA name must also appear on the physical label. The PHYSICALMEDIA naming scheme should start with a 2 or 3 letter prefix (identifying your company) followed by a 3-digit counter (e.g., ABC001). Each separate volume delivered on that media must also have a separate VOLUMENAME associated with it. On the root of the media, the top level folder(s) must be named for the volume(s). VOLUMENAME(s) should also be indicated on the physical label of the media. The volume naming scheme should be based on the PHYSICALMEDIA name followed by a hyphen, followed by a 3-digit counter (e.g., ABC001001). The VOLUMENAME should increase sequentially across all productions on the same PHYSICALMEDIA. Under the VOLUMENAME folder, the production should be organized in 4 subfolders:

1. DOCLINK (contains linked native files, may contain subfolders, with no more than 5,000 files per folder)
2. IMAGES (may contain subfolders, with no more than 5,000 image files per folder)
3. FULLTEXT (may contain subfolders, with document-level text files)
4. LOADFILES (should contain the metadata, DII, OPT, LST, and custodian append files)

G. **Deliverables**

The AGO accepts electronic productions loaded onto hard drives, USB drive, CD-ROMs, or DVD-ROMs. Each piece of media a unique identifier (PHYSICALMEDIA) must be provided and should also be physically visible on the exterior of the physical item. Should you wish to make a production by electronic transfer, please discuss with the AGO in sufficient time prior to your production.

All deliverables should identify, at a minimum, the following:

1. Case number
2. Production date
3. Producing party
4. Bates Range

If the media is encrypted, please supply the tool for decryption on the same media, and instructions for decryption. A separate email or letter must be sent with the password to decrypt.

All documents produced in electronic format shall be scanned for, and free of, viruses. The AGO will return any infected media for replacement.

IMAGE and TEXT FILE SPECIFICATIONS, & LOAD FILE CONFIGURATION

Image/Native File Specifications

- Black-and-white Group IV Single-Page TIFFs (300 DPI). Color images should be provided in .JPG format when color is necessary.
- Image file names should match the page identifier for that specific image and end with the .tif (or .jpg if needed) extension.
- File names and folder names should not contain embedded spaces or special characters (including the comma).
- Images for a given document must reside together in the same folder.
- Native file names should match the PRODBEG for that specific record and end with the appropriate file extension.
- Native files should have a placeholder image numbered by the PRODBEG of the file and at a minimum contain the PRODBEG and FILENAME.
- All files must have a unique bates number.
- All images must be endorsed with sequential Bates numbers in the lower right corner of each image.
- Any encryption or password protection will be removed from all native format files produced.

Searchable Text File Specifications and Control List Configuration

- Extracted text should be provided with all records, except for documents that originated as hard copy or redacted documents.
  - For hard copy documents, please provide OCR text.
  - For redacted documents, provide OCR text for the redacted version.
- Text must be produced as separate text files, not as fields within the .DAT file. The full path to the text file (OCRPATH) should be included in the .DAT file. We require document level ANSI text files, named per the BATESBEG/Image Key. Please note in the cover letter if any non-ANSI text files are included in the production. Extracted text files must be in a separate folder. There should be no special characters (including commas in the folder names). For redacted documents, provide the full text for the redacted version.

Metadata Load File Delimiters and Configuration

- Field Separator = Column (ASCII 020)
- String value delimiter = Quote (ASCII 254)
- Newline delimiter = (ASCII 174)
- Multi-value separator = (ASCII 059)
- Date format YYYYMMDD (date type fields only)
- Time format HH:MM:SS

Opticon Image Load File (.opt) Configuration – Page level comma-delimited file containing seven fields per line.
PageID,VolumeLabel,ImageFilePath,DocumentBreak,FolderBreak,BoxBreak,PageCount

- PageID – PageID of the item being loaded. MUST be identical to the image name (less the file extension).
- VolumeLabel – Optional. If used it is preferable that it match the VOLUMENAME assigned in the corresponding metadata load file.
- ImageFilePath – The path to the image from the root of the delivery media.
- DocumentBreak – The letter "Y" denotes the first page of a document. If this field is blank the page is not the first page of a document.
- FolderBreak – Leave empty
- BoxBreak – Leave empty
- PageCount – Optional
- Example - EXP-0000001,\ABC001\Images\001\ ABC0000001.tif,Y,,,

The metadata of electronic document collection should be extracted and provided in a .DAT file using the field definition and formatting described below:

Field Name	Sample Data	Description
PRODUCING PARTY	Company XYZ; John Smith	Producing Party Name
PHYSICALMEDIA	ABC001	Unique identifier for that media
VOLUMENAME	ABC001-001	Production volume number
CUSTODIAN	Smith, John; XYZ Dept.	Custodian(s) and/or source information
HASHMD5 (or SHA-1)	d41d8cd98f00b204e9800998ecf8427e	MD5 (or SHA-1) hash value used for de-duplication or other processing
PRODBEG	EXP0000001	Starting Bates number per document
PRODEND	EXP0000001	Ending Bates number per document
PRODBEGATTACH	EXP0000001	First Bates number of a single attachment
PRODENDATTACH	EXP0000001	Last Bates number of a single attachment
ATTACHRANGE	EXP0000001-EXP0000009	Bates range from the first page of the parent document to the last page of the last child document
PARENTBATES	EXP0000001	First Bates number of a parent document/email; this field should be populated for each child document.
CHILDBATES	EXP0000002; EXP0000007	First Bates number of each child attachment; can be more than one Bates number if multiple attachments; this field should be populated for each parent document.
FROM	John Smith; john.smith@abcco.com	Email sender
TO	John Smith; john.smith@abcco.com	Email recipient(s); semi-colons should separate multiple entries
CC	John Smith; john.smith@abcco.com	Email carbon copy(s); semi-colons should separate multiple entries
BCC	John Smith; john.smith@abcco.com	Email blind carbon copy(s) semi-colons should separate multiple entries
SUBJECT	Your Subject Here	Email Subject Line
FILENAME	YourFilenameHere.doc	The original native file, including extension
DATESENT	YYYYMMDD	Date email sent
TIMESENT	HH:MM:SS	Time email sent
TIMEZONE	CST	The time zone in which emails were standardized during conversion
TIMERECEIVED	HH:MM:SS	Time email received
AUTHOR	John Smith	Author of a document
DATECREATED	YYYYMMDD	Date the document was created.
TIMECREATED	HH:MM:SS	Time
DATE LAST MODIFIED	YYYYMMDD	Date document was last modified
FILEEXTENSION	.msg; .doc; .xls; .ppt	File extension of native document
FILE SIZE	550 MB; 2GB	File size in bytes
PGCOUNT	2	Number of pages in native file or email
FILEPATH	P:\shared\smithj\yourfilenamehere.doc	Path where native file document was stored, including original filename
OCRPATH	Text/001/EXP0000001.txt	Path to extracted text
PROPERTIES	Redacted; Attorney-Client Privilege	Privilege notation, Redacted, Document withheld based on privilege