UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

NEURAL MAGIC, INC.,

Plaintiff,

v.

FACEBOOK, INC. and ALEKSANDAR ZLATESKI,

Defendants.

Civil Action No. 1:20-cv-10444-DJC

~~[PROPOSED]~~ STIPULATED ESI ORDER

WHEREAS, all the parties to this action (collectively the "Parties" and individually a "Party") request that this Court issue an order governing discovery of electronically stored information ("ESI"), as a supplement to the Federal Rules of Civil Procedure and any other applicable orders and rules;

WHEREAS, the Parties, through counsel, agree to the following terms; and

WHEREAS, this Court finds good cause exists for issuance of an appropriately tailored ESI order,

IT IS HEREBY ORDERED that any person subject to this Order – including without limitation the Parties to this action (including their respective corporate parents, successors, and assigns), their representatives, agents, experts and consultants, all third parties providing discovery in this action, and all other interested persons with actual or constructive notice of this Order — will adhere to the following terms:

1. This Order supplements all other discovery rules and orders. It streamlines ESI production to promote a "just, speedy, and inexpensive determination" of this action, as required by the Federal Rules of Civil Procedure.

2. This Order does not cover the production of computer code, which is governed by a separate Protective Order. *See* D.I. 52.

3. This Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown. If the Parties cannot resolve disagreements regarding modifications, they will submit their disputes to the Court in accordance with the Court's rules, practices, and orders.

4. For purposes of this Order, Plaintiff Neural Magic, Inc. ("NMI") will be considered one "Party," and Defendants Facebook, Inc. ("Facebook") and Dr. Aleksandar Zlateski, together, will be considered another "Party."

5. Cooperation and Proportionality. The Parties are aware of the importance the Court places on cooperation and commit to cooperate in good faith throughout this matter. The Parties agree to use reasonable, good faith, and proportional efforts to preserve, identify, and produce relevant and discoverable information consistent with Fed. R. Civ. P. 26(b)(1). This includes identifying appropriate limits to discovery, including limits on custodians, identification of relevant subject matter, time periods for discovery, and other parameters to limit and guide preservation and discovery issues. For example, the Parties agree that in responding to an initial Fed. R. Civ. P. 34 request, or earlier if appropriate, they will meet and confer about methods to search ESI in order to identify ESI that is subject to production in discovery and filter out ESI that is not subject to discovery. The failure of counsel or the parties to cooperate in facilitating and reasonably limiting e-discovery requests and responses will be considered in cost-shifting determinations.

6. Preservation. Each Party is responsible for taking reasonable and proportionate steps to preserve relevant and discoverable ESI within its possession, custody or control consistent with Sedona Conference Principle 6 which instructs that "[r]esponding parties are best

situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information."[1] The Parties have discussed their preservation obligations and needs and agree that preservation of relevant ESI will be reasonable and proportionate. To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the parties agree that:

(a) Parties shall preserve non-duplicative, relevant information currently in their possession, custody, or control; however, Parties are not be required to modify, on a going-forward basis, the procedures used by them in the usual course of business to back up and archive data; and

(b) The following data sources are not reasonably accessible because of undue burden or cost pursuant to Fed. R. Civ. P. 26(b)(2)(B), and ESI from these sources will be preserved pursuant to normal business retention, but not searched, reviewed, or produced, unless otherwise ordered by the Court upon a motion of a party:

i. backup systems and/or tapes used for disaster recovery; and

ii. systems no longer in use that cannot be accessed by using systems currently in use by the Party.

(c) The Parties agree not to preserve, collect, process, review and/or produce the following data types from any source regardless of relevance:

i. Deleted, slack space, fragmented, or unallocated data only accessible by additional forensics beyond those undertaken in the normal course, but to the extent upon reasonable search and collection efforts either party becomes aware of any relevant materials that have been deleted and cannot be recovered other than

[1] The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 19 SEDONA CONF. J. 118 (2018).

by additional forensics not already being undertaken as required to conduct a reasonable search and collection, such party shall notify the other party within 5 days. The notifying Party will make its best efforts to preserve any such materials for 10 days or until the notified Party either consents to preserved materials no longer being preserved or requests that such materials be preserved so that the notified Party can seek relief from the Court. If such relief is sought, preserved materials shall continue to be preserved by the notifying Party until the issue is resolved by the Court.

ii. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

iii. Temporary internet files, history, cache, and cookies.

iv. Data in metadata fields that are frequently updated automatically, such as last-opened or last modified dates.

v. Server, system, or network logs.

vi. Dynamic fields in databases or log files not stored or retained in the usual course of business.

vii. Information created or copied during the routine, good-faith performance of processes for the deployment, maintenance, retirement, and/or disposition of computer equipment by the party.

viii. Other forms of ESI whose preservation requires unreasonable, disproportionate, and/or non-routine, affirmative measures that are not utilized in the ordinary course of business.

7. General production requests under Federal Rules of Civil Procedure 34 and 45 will include email or other forms of electronic correspondence (collectively "email"); however,

for the avoidance of doubt, the Parties note here and agree that custodian-specific data (both email and other custodial data) will be collected, searched, and produced in accordance with Paragraphs 8 and 9 below, which govern "Custodians" and "Search Terms and Email Discovery," respectively.

8. Custodians. A requesting Party can request the collection, search, and production of data (both email and other custodial data) from up to a total of seven (7) custodians from a producing Party. Proposed custodians shall initially be identified by the producing Party, and as noted above, the Parties will seek to cooperate to identify the seven (7) custodians per Party for custodian-specific discovery. The Parties may jointly agree to modify this limit without the Court's leave. The Court may consider contested requests for additional custodians per side, upon a showing of good cause.

9. Search Terms and Email Discovery:

(a) The Parties shall timely attempt to reach agreement on search terms for searches of custodian-specific data (both email and other custodial data), or a computer- or technology-aided methodology, and will continue to cooperate in revisiting the search terms or computer or technology-aided methodology.

(b) Each requesting Party is limited to seven (7) search terms per custodian (for both email and other custodial data), which shall initially be identified by the requesting Party. The Parties may jointly agree to modify the seven (7) search terms per custodian limit without the Court's leave. The Court may consider contested requests for additional search terms per custodian, upon a showing of good cause.

(c) The Parties will seek to tailor search terms to particular issues, and will meet and confer to provide feedback on the number of hits of proposed search terms. The Parties also will seek to limit requests for custodian-specific data (both email and other custodial data) to proper timeframes.

(d) Notwithstanding the foregoing provisions relating to search terms, each Party will make reasonable efforts to engage in collection efforts prior to the finalization of search terms, and the Parties' development and negotiation of search terms for custodial email and other ESI will not be grounds for a Party to delay the review, collection, or production of non-custodial or other documents that the producing Party is able to identify and locate without undue burden and without the use of search terms. The Parties note here, for the avoidance of doubt, that each Party is required to collect and produce relevant documents that can be identified and located, without undue burden, without the use of search terms, regardless of whether agreed-to search terms capture such documents.

(e) Nothing in this Order may be construed or interpreted as precluding a producing party from performing a responsiveness review to determine if documents captured by search terms are in fact relevant to the requesting party's request. Similarly, nothing may be construed or interpreted as precluding a producing party from performing a privilege review of documents determined to be relevant by any means. Further, nothing in this Order shall be construed or interpreted as requiring the production of all documents captured by any search term if one or more of such documents are in good faith and reasonably deemed not relevant to a requesting Party's request or privileged.

(f) Each party will use its best efforts to filter out common system files and application executable files by using a commercially reasonable hash identification process. For example, hash values that may be filtered out during this process are located in the National Software Reference Library ("NSRL") NIST hash set list.

(g) Email Threading. Where multiple email messages are part of a single chain or "thread," a Party is only required to produce the most inclusive message ("Last In Time Email") and need not produce earlier, less inclusive email messages or "thread members" that are fully contained, including attachments and including identical senders and recipients, within the Last In Time Email. Only email messages for which the parent document and all attachments are contained in the Last In Time Email will be considered less inclusive email messages that need not be produced.

10. Production protocol. The Parties agree to produce documents in the formats described in Appendix A to this Order. If particular documents warrant a different format, the parties will cooperate to arrange for the mutually acceptable production of such documents. The parties agree to prevent, to the extent possible, materially degrading the searchability of documents as part of the document production process.

11. Privilege logs:

(a) Consistent with the Federal Rules of Civil Procedure, a Party withholding or redacting any responsive document on the grounds of privilege, immunity, or any similar claim shall provide to the receiving Party a privilege log, except:

i. No Party is required to identify on its respective privilege log any document or communication dated after the filing of the Complaint. [#52 ¶ 14.5];

ii. documents concerning activities undertaken to comply with the duty to preserve information (including, but not limited to, litigation hold letters) that are protected from disclosure under Fed. R, Civ. Proc. 26(b)(3)(A) and (B) need not be included in the privilege log.

iii. the Parties agree to log only the Last In Time Emails in a thread and need not log earlier, less inclusive email messages or "thread members" that are fully contained within the Last In Time Email.

iv. Communications for the time period January 22, 2020 to the filing of the Complaint may be identified on a privilege log by category, rather than individually, if appropriate.

(b) For any document withheld or redacted, the relevant privilege log will contain the following information: (i) the date of the document; (ii) the identity of all persons who authored, signed, or otherwise prepared the document; (iii) the identity of all persons designated as addressees; (iv) a description of the contents of the document that, without revealing information itself privileged or protected, is sufficient to understand the subject matter of the document and the basis of the claim of privileged or immunity; (v) the type or nature of the privilege asserted (e.g., attorney-client privilege, work product doctrine, etc.); and (vi) for redacted documents only, the bates numbers corresponding to the first and last page of any document redacted. For all individuals listed on a log whose role as an attorney is the basis for a claim of privilege, the privilege log will contain some indication that the individual is an attorney (for example, an asterisk next to each attorney's name).

12. Deduplication. A Party is only required to produce one copy of each responsive document and a Party may de-duplicate responsive ESI (based on MD5 or SHA-1 hash values at the document level) on a global scale, as long as the producing Party provides information identifying the other custodians who possessed any given record or ESI, for example, in a "custodian" meta data field. Alternatively, a Party may elect to de-duplicate each custodian's responsive ESI and may de-duplicate the Party's non-custodial ESI (based on MD5 or SHA-1 hash values at the document level). To the extent emails are produced, the following procedures will apply. For emails with attachments, the hash value is generated based on the parent/child document grouping. To the extent that de-duplication through MD5 or SHA-1 hash values is not possible, the Parties will meet and confer to discuss alternative methods of deduplication.

13. The Parties consent to service via electronic means (e.g., via email), consistent with Fed. R. Civ. P. 5(b)(2)(B)(E).

14. Nothing in this Order requires disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work-product doctrine, or any other applicable privilege or immunity.

15. The parties do not waive any objections to the production, discoverability, admissibility, or confidentiality of documents and ESI.

IT IS SO STIPULATED, THROUGH COUNSEL OF RECORD.

Dated: November 13, 2020

/s/ Patrick Curran
Patrick D. Curran (BBO No. 568701)
Steven Cherny (BBO No. 706132)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
111 Huntington Avenue, Suite 520
Boston, MA 02199
Telephone: (617) 712-7100
stevencherny@quinnemanuel.com
patrickcurran@quinnemanuel.com

Attorneys for Plaintiff
NeuralMagic, Inc.

Dated: November 13, 2020

/s/ Christopher W. Henry
Christopher W. Henry (BBO No. 676033)
William J. Trach (BBO No. 661401)
Nathanial J. McPherson (BBO No. 697666)
LATHAM & WATKINS LLP
John Hancock Tower
200 Clarendon Street, 27th Floor
Boston, MA 02116
(617) 948-6000 / (617) 948-6001 Fax
william.trach@lw.com
christopher.henry@lw.com
nathanial.mcpherson@lw.com

Douglas E. Lumish (*pro hac vice*)
LATHAM & WATKINS LLP
140 Scott Drive
Menlo Park, CA 94025
(650) 328-4600 / (650) 463-2600 Fax
douglas.lumish@lw.com
Jennifer L. Barry (*pro hac vice*)
LATHAM & WATKINS LLP
12670 High Bluff Drive
San Diego, CA 92130
(858) 523-5400 / (858) 523-5450 Fax
jennifer.barry@lw.com

Attorneys for Defendant
Facebook, Inc.

/s/ Stephen D. Riden
Stephen D. Riden (BBO No. 644451)
Russell Beck (BBO No. 561031)
Hannah T. Joseph (BBO No. 688132)
BECK REED RIDEN LLP
155 Federal Street, Suite 1302
Boston, MA 02110
(617) 500-8660 / (617) 500-8665 Fax
rbeck@beckreed.com
sriden@beckreed.com
hjoseph@beckreed.com

Attorneys for Defendant
Aleksandar Zlateski

PURSUANT TO THE PARTIES' STIPULATION, IT IS SO ORDERED.

DATED: November 16, 2020

Denise J. Casper

Hon. Denise Casper
United States District Judge

APPENDIX A: PRODUCTION PROTOCOL

1. **Production Components.** Except as otherwise provided below, ESI shall be produced in accordance with the following specifications:

   (a) an ASCII delimited data file (.DAT) using standard delimiters;

   (b) an image load file (.OPT) that can be loaded into commercially acceptable production software (*e.g.* Concordance);

   (c) TIFF images;

   (d) and document level .TXT files for all documents containing extracted full text or OCR text.

   (e) Parent-child relationships will be maintained in production.

   If a particular document warrants a different production format, the parties will cooperate in good faith to arrange for a mutually acceptable production format.

2. **Production Media and Access Controls.** Documents shall be encrypted and produced through electronic means, such as secure file sharing methods (*e.g.* FTP), or on CD, DVD, flash drive or external hard drive ("Production Media"). Each piece of Production Media shall identify a production number corresponding to the production volume (*e.g.* "VOL001"). Each piece of Production Media shall also identify: (a) the producing party's name; (2) the production date; (3) the Bates Number range of the materials contained on the Production Media.

   Nothing in this ESI Order will preclude or impair any and all protections provided the parties by the Protective Order in this case. D.I. 52. Any data produced by the producing party must be protected in transit, in use, and at rest by all in receipt of such data. Parties will use best efforts to avoid the unnecessary copying or transmittal of produced documents. Any copies made of produced data must be kept on media or hardware employing whole-disk or folder level encryption or otherwise secured on information systems and networks in a manner consistent with the best practices for data protection. If questions arise, Parties will meet and confer to ensure security concerns are addressed prior to the exchange of any documents.

3. **Data Load Files/Image Load Files.** Each TIFF in a production must be referenced in the corresponding image load file. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the image load file(s) in the production. The total number of pages referenced in a production's image load file should match the total number of TIFF files in the production. All images must be assigned a unique Bates number that is sequential within a given document and across the production sets. The Bates Numbers in the image load file must match the corresponding documents' beginning Bates numbers in the data load file. The total number of documents in a production should match the total number of records in the data load file. Load files shall not vary in format or structure within a production, or from one production to another.

4. **Metadata Fields.** Each of the metadata and coding fields set forth below that can be extracted shall be produced for each document. The parties are not obligated to populate manually any of the fields below if such fields cannot be extracted from a document, with the exception of the following: (a) BEGBATES, (b) ENDBATES, (c) BEGATTACH, (d) ENDATTACH, (e) CUSTODIAN, (f) DEDUPED_CUSTODIAN, (g) CONFIDENTIALITY, (h) REDACTIONS, (i) NATIVEFILEPATH, (j) TEXTFILEPATH, and (k) HASHVALUE, which should be populated by the party or the party's vendor. The parties will make reasonable efforts to ensure that metadata fields automatically extracted from the documents correspond directly to the information that exists in the original documents.

Field Name	Field Description
BEGBATES	Beginning Bates number as stamped on the production image
ENDBATES	Ending Bates number as stamped on the production image

Field Name	**Field Description**
BEGATTACH	First production Bates number of the first document in a family
ENDATTACH	Last production Bates number of the last document in a family
ALLCUSTODIAN(S)	Individual(s) from whom the documents originated
CONFIDENTIALITY	Confidentiality designation assigned to document
NATIVEFILEPATH	Native File Link (Native Files only)
TEXTFILEPATH	Path to extracted text/OCR file for document
HASHVALUE	MD5 hash value of document
AUTHOR	Any value populated in the Author field of the document properties (Edoc or attachment only)
DOCDATE	Date the document was created (format: MM/DD/YYYY) (Edoc or attachment only)
DATEMODIFIED	Date when document was last modified according to filesystem information (format: MM/DD/YYYY) (Edoc or attachment only)
FROM	The name and email address of the sender of the email
TO	All recipients that were included on the “To” line of the email
CC	All recipients that were included on the “CC” line of the email
BCC	All recipients that were included on the “BCC” line of the email
DATERECEIVED	Date email was received (format: MM/DD/YYYY)
DATESENT	Date email was sent (format: MM/DD/YYYY)
FILESIZE	The original file size of the produced document
REDACTED	Indicate Yes/No if document redacted

5. **TIFFs.** Documents that exist only in hard copy format shall be scanned and produced as TIFFs. Documents that exist as ESI shall be converted and produced as TIFFs, except as provided below. The parties shall take reasonable efforts to process presentations (*e.g.*

MS PowerPoint) with hidden slides and speaker's notes unhidden, and to show both the slide and the speaker's notes on the TIFF image. Unless excepted below, single page, black and white, Group IV TIFFs should be provided, at least 300 dots per inch (dpi) for all documents. Each TIFF image shall be named according to a unique corresponding Bates number associated with the document. Each image shall be branded according to the Bates number and the agreed upon confidentiality designation. Original document orientation should be maintained (i.e., portrait to portrait and landscape to landscape). Where the TIFF image is unreadable or has materially degraded the quality of the original, the producing party shall provide a higher quality TIFF image or the native or original file.

6. **Color.** The parties may request color copies of a limited number of documents where color is necessary to accurately interpret the document.

7. **Text Files.** A single multi-page text file shall be provided for each document, and the filename should match its respective TIFF filename. When possible, the text of native files should be extracted directly from the native file. Text files will not contain the redacted portions of the documents. A commercially acceptable technology for optical character recognition "OCR" shall be used for all scanned, hard copy documents and for documents with redactions.

8. **Native files.** Spreadsheets (*e.g.* MS Excel) will be produced in native format unless redacted, in which instance, spreadsheets shall be produced in TIFF with OCR Text Files. To the extent that they are produced in this action, audio, video, and multi-media files will be produced in native format. Native files shall be produced with a link in the NATIVEFILEPATH field, along with extracted text (where extracted text is available) and applicable metadata fields set forth in paragraph 4 above. A Bates numbered TIFF placeholder indicating that the document was provided in native format must accompany every native file.

9. **Confidentiality Designation.** Responsive documents in TIFF format will be stamped with the appropriate confidentiality designations in accordance with the protective order entered in this matter. D.I. 52. Each responsive document produced in native format will have its confidentiality designation identified in the filename of the native file and indicated on its corresponding TIFF placeholder.

10. **Databases and Other Structured Data.** The parties shall meet and confer regarding the production format and scope of data contained in databases in order to ensure that any information produced is reasonably usable by the receiving party and that its production does not impose an undue burden on the producing party, by, for example, requiring development of reports and/or software code to extract the information. To avoid doubt, information will be considered reasonably usable when produced in CSV format, tab-delimited text format, Microsoft Excel format, or Microsoft Access format. To the extent a party is constrained from producing responsive ESI because of a third-party license or because software necessary to view the ESI is hardware-dependent, the parties shall meet and confer to reach an agreement on alternative methods to enable the requesting party to view the ESI.