182 3107

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of **Cambridge Analytica, LLC,** **a corporation.**	**DOCKET NO. 9383**

COMPLAINT

The Federal Trade Commission, having reason to believe that Cambridge Analytica, LLC, a corporation, ("Respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

NATURE OF THE CASE

1. This action seeks to hold Respondent responsible for its deceptive acts and practices to harvest personal information from Facebook users for political and commercial targeted advertising purposes. Respondent, along with Alexander Nix and Aleksandr Kogan, jointly and severally, developed, operated, analyzed, and used data obtained through an application on the Facebook platform called the "GSRApp," also sometimes referred to publicly as the "thisisyourdigitallife" app. Using the Graph application programming interface ("Graph API") Facebook made available to developers on its platform, the GSRApp harvested Facebook user profile data from approximately 250,000–270,000 Facebook users who directly interacted with the app, as well as 50–65 million of the "friends" in those users' social networks. Cambridge Analytica, LLC, Alexander Nix, and Aleksandr Kogan obtained the app users' consent to collect their Facebook profile data through false and deceptive means. Specifically, they falsely represented that the GSRApp did not collect any identifiable information from the Facebook users who authorized it.

RESPONDENT

2. Respondent Cambridge Analytica, LLC ("Cambridge Analytica") is a private Delaware limited liability company that was formed in December 2013, and had a principal office or place of business at 597 Fifth Avenue, 7th Floor, New York, NY 10017. Cambridge

Analytica is part of the SCL Group Ltd. family of companies. SCL Elections Limited ("SCL Elections"), a privately held U.K. Corporation, has held an ownership interest in Cambridge Analytica. Cambridge Analytica has operated as a data analytics and consulting company that provides voter-profiling and marketing services. Cambridge Analytica describes itself on its website as "a data-science consultancy and marketing agency" that is "politically neutral." In May 2018, Cambridge Analytica filed for bankruptcy, which proceedings are still ongoing.

3. During the relevant time period, Cambridge Analytica and SCL Elections conducted the business practices described below through an interrelated network of companies that have common business functions, ownership, officers, and employees. For example, Alexander Nix was both the head of SCL Elections and also the Chief Executive Officer of Cambridge Analytica. SCL Elections was placed into liquidation on April 17, 2019.

RELATED PARTIES

4. Aleksandr Kogan ("Kogan") is an American citizen currently residing in New York. Until September 2018, Kogan was a Senior Research Associate and Lecturer at the Department of Psychology at the University of Cambridge in the United Kingdom, where he established and led the Cambridge Prosociality and Well-Being Lab ("CPW Lab"). Kogan was also an owner and co-founder of the now-defunct U.K. corporation, Global Science Research, Ltd. ("GSR"). Kogan has been known at times by the married name, Aleksandr Spectre.

5. Alexander James Ashburner Nix ("Nix") is a British citizen currently residing in the United Kingdom. Until April 30, 2018, Nix was the Chief Executive Officer of Cambridge Analytica and also a director of SCL Elections. Individually or in concert with others, Nix formulated, directed, controlled, had the authority to control, or participated in the acts and practices alleged in this complaint. Nix currently resides in London, England. Nix, in connection with the matters alleged herein, transacts or has transacted business throughout the United States.

JURISDICTION

6. The acts or practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, and constitute "deceptive acts or practices involving foreign commerce" as set forth in Section 5 of the FTC Act.

RELEVANT BUSINESS PRACTICES

A. Agreement to Harvest Facebook User Profile Data for Commercial Purposes

7. In late 2013 or early 2014, Nix, SCL Elections, and Cambridge Analytica became aware of research by individuals at the Psychometrics Centre within the University of Cambridge that found that Facebook profile information could be used to successfully predict an

individual's personality traits according to the "OCEAN" scale, a psychometric model that measures an individual's openness to experiences, conscientiousness, extraversion, agreeableness, and neuroticism.

8. Specifically, researchers developed an algorithm that could predict an individual's personality based on the individual's "likes" of public Facebook pages. For example, liking Facebook pages related to *How to Lose a Guy in 10 Days*, George W. Bush, and rap and hip-hop could be linked with a conservative and conventional personality. The researchers argued that their algorithm, which was more accurate for individuals who had more public Facebook page "likes," could potentially predict an individual's personality better than the person's co-workers, friends, family, and even spouse.

9. Nix, SCL Elections, and Cambridge Analytica were interested in this research because Cambridge Analytica intended to offer voter profiling, microtargeting, and other marketing services to U.S. campaigns and other U.S.-based clients. Through mutual contacts, representatives of SCL Elections (who had dual roles at Cambridge Analytica) reached out to Kogan and academics affiliated with the Psychometrics Centre in early 2014 to discuss a potential working relationship to commercialize this research.

10. Kogan had expertise researching and analyzing Facebook data through his work at the CPW Lab, as well as his prior research collaborations with Facebook that analyzed aggregated Facebook data relating to how people worldwide connect and express emotions. Kogan was willing to enter into a commercial venture with SCL Elections, and after several months of discussion, the parties reached agreement about the scope of work (the "Project").

11. Importantly, Kogan already had a Facebook app that was registered on the Facebook platform, the CPW Lab app, that could be repurposed to collect profile data from Facebook users and their "friends" through Facebook's developer tool, Graph API (v.1).

12. Facebook's Graph API (v.1) allowed developers to collect Facebook profile data from users who directly installed or otherwise interacted with the developer's application or website through a Facebook Login ("App Users"), as well as from these users' Facebook "friends." Facebook allowed this data collection even though the "friends" did not have any direct interaction with the app or website ("Affected Friends"). While Facebook had announced in April 2014 that it was introducing a new version of the Graph API—v.2—that would no longer allow developers to collect profile data from Affected Friends, only from the App Users themselves, existing apps had one year before these limitations went into effect, whereas new apps would automatically be limited. Kogan's app was, thus, "grandfathered" into the more permissive data collection allowable under Graph API (v.1), making Kogan an appealing partner for Nix, Cambridge Analytica, and SCL Elections.

13. On May 29, 2014, Kogan incorporated GSR to carry out the Project, separate and apart from his duties at the University of Cambridge. Kogan was the Chief Executive Officer of GSR at all relevant times, and worked on all aspects of GSR's products and services before it was dissolved in October 2017.

14. On June 4, 2014, GSR and SCL Elections entered into a GS Data and Technology Subscription Agreement (the "June 2014 Agreement"). Nix signed this agreement for SCL Elections. Under this agreement, GSR agreed to harvest Facebook profile data from App Users and Affected Friends in 11 U.S. states, generate personality scores for these individuals, and then match these profiles to U.S. voter records provided to GSR by SCL Elections. GSR would then send these matched records along with the associated personality scores back to SCL Elections. GSR retained the original data set and granted SCL Elections a license to access the data and to use the proprietary GSR personality scores. Following the creation of GSR and the signing of the June 2014 Agreement, Kogan repurposed the CPW Lab app to become the "GSRApp."

15. Although SCL Elections is the entity that entered into the agreement with GSR, it was acting for and on behalf of Cambridge Analytica. SCL Elections entered into a Services Agreement with Cambridge Analytica whereby SCL Elections agreed, among other things, to (a) acquire, for and on behalf of Cambridge Analytica, demographic, transactional, lifestyle, and behavioral data about consumers in target populations; (b) identify and build target voter lists; (c) apply research techniques to understand better the habits and daily lives of target voter groups; and (d) apply psychological profiles to target groups of voters. In a separate agreement, SCL Elections also agreed to license all of its intellectual property to Cambridge Analytica.

16. SCL Elections and Cambridge Analytica played a significant and direct role in the development and implementation of the GSRApp, as well as in the analysis of the data the GSRApp collected. For example:

    a. SCL Elections and Cambridge Analytica revised the terms of use for the GSRApp from the original CPW Lab app;

    b. SCL Elections and Cambridge Analytica paid all costs—totaling over five hundred thousand dollars—related to implementing the GSRApp and analyzing the resulting data, including paying U.S.-based survey panel providers to specifically target Facebook users located in the United States to take the GSRApp surveys;

    c. SCL Elections and Cambridge Analytica inserted specific questions to be included in some of the surveys, including a number of questions about national security in the United States because this was a particular topic of interest for one of Cambridge Analytica's U.S.-based clients;

    d. SCL Elections and Cambridge Analytica directly communicated with the U.S.-based survey panel provider about the timing and focus of the GSRApp surveys; and

    e. SCL Elections and Cambridge Analytica actively assisted in the matching of data harvested from App Users and Affected Friends located in the U.S. and Kogan's personality scores with U.S. voter registration records.

17. Nix was personally involved in the data harvesting Project. In addition to signing the June 2014 Agreement, he directly communicated and met with Kogan about the Project, personally authorized payment for Project-related costs, reviewed survey questions and specifically requested certain Facebook data or analysis, and directed internal actions within SCL Elections and Cambridge Analytica related to implementing the GSRApp, analyzing the GSRApp data, and using the GSRApp data for Cambridge Analytica clients in the United States.

B. The GSRApp Harvested Large Quantities of Facebook Profile Data from App Users and Affected Friends Through False and Deceptive Means

18. The GSRApp asked users to answer survey questions and consent to their Facebook profile data being collected, including public Facebook page "likes." Kogan then used the initial participants' survey responses and Facebook "likes" to train his algorithm so that it could predict the users' personality traits based solely on the Facebook "likes" data. This process, which was inspired by original research by others at the University of Cambridge, allowed Kogan to provide personality scores for the Affected Friends, from whom he collected Facebook data but had no survey responses.

19. Kogan then assigned a confidence level to each personality score based on the number of public page "likes" for each U.S.-based App User and Affected Friend, generally requiring a Facebook user to have "liked" at least 10 public Facebook pages to be confident of the personality score.

20. Cambridge Analytica, Nix, and Kogan then conducted a small trial to determine how well Facebook profile information could be matched with U.S. voter records and information from other public databases. The Project would have little value to SCL Elections and Cambridge Analytica if the personality scores could not be matched with actual U.S. voters.

21. The initial trial was a success and showed that the Facebook profile data could be matched with U.S. voter records. Based on this success, Cambridge Analytica, Nix, and Kogan implemented the GSRApp on a wider scale using the Qualtrics survey platform, based in Provo, Utah.

22. Qualtrics recruited U.S.-based consumers through four waves of survey panels over the summer of 2014. Each wave asked different questions of the participants such that Kogan's personality scores covered a broad range of topics, including political enthusiasm, political orientation, frequency in voting, consistency in voting for the same political party, and views on particular controversial issues. Survey participants who completed the survey and authorized the GSRApp to harvest their Facebook profile information were paid a nominal fee of a few dollars for participating in the survey.

23. At the point in every survey in which the GSRApp asked U.S. consumers to authorize the app to collect their Facebook data, the GSRApp made the following representation:

> In this part, we would like to download some of your Facebook data using our Facebook app. We want you to know that we will NOT download your name or any other identifiable information—we are interested in your demographics and likes.

24. Contrary to this representation, the GSRApp collected the Facebook User ID of those users who authorized it. A Facebook User ID is a persistent, unique identifier that connects individuals to their Facebook profiles. Cambridge Analytica, Nix, and Kogan included this representation after finding that half of the survey participants initially refused to grant the GSRApp permission to collect their Facebook profile data.

25. Cambridge Analytica, Nix, and Kogan harvested a significant amount of Facebook profile data from App Users and the Affected Friends located in the U.S. through the GSRApp. Specifically, they harvested the following Facebook profile data from App Users: Facebook User ID; gender; birthdate; location ("current city"); friends list; and "likes" of public Facebook pages. They harvested from Affected Friends their Facebook User ID; name; gender; birthdate; location ("current city"); and "likes" of public Facebook pages.

26. Over the course of the Project, Cambridge Analytica, Nix, and Kogan harvested Facebook profile data from approximately 250,000–270,000 App Users located in the U.S., and harvested profile data from approximately 50–65 million Affected Friends, including at least 30 million identifiable U.S. consumers.

27. In January 2015, GSR and SCL Elections entered into a supplemental agreement ("January 2015 Agreement") regarding additional data from the Project that SCL Elections and Cambridge Analytica wanted. Pursuant to the January 2015 Agreement, GSR provided data and analysis for App Users and Affected Friends for the remaining 39 U.S. states. GSR also provided a more limited set of personality analyses for these consumers than it had provided for consumers in the initial 11 U.S. states.

28. In April 2015, GSR and SCL Elections entered into an addendum to the January 2015 Agreement ("Addendum"), pursuant to which GSR provided SCL Elections and Cambridge Analytica with the underlying Facebook data used to "train" the algorithm that generated the OCEAN personality scores. GSR also provided SCL Elections and Cambridge Analytica with additional information about whether the App Users and Affected Friends included in the second set of data provided pursuant to the January 2015 Agreement had "likes" for about 500 specific pages identified by SCL Elections and Cambridge Analytica.

29. Nix, SCL Elections, and Cambridge Analytica reported to Kogan that they had very positive feedback from their clients and had expressed an interest in continuing to work with Kogan and GSR on other similar projects. While Kogan and GSR were interested in working on follow-up projects, the parties could not reach an agreement and discontinued their work together after GSR transferred the data agreed to in the Addendum in May 2015.

30. In December 2015, several news reports were published regarding Cambridge Analytica's use of Facebook data. Following these reports, Facebook demanded that Kogan, Cambridge

Analytica, and its SCL affiliates delete all Facebook data in their possession. While Kogan and SCL Elections certified to Facebook that they had deleted the data obtained through the GSRApp, individuals or other entities still possess this data and/or data models based on this data.

C. Cambridge Analytica Deceptively Claimed it Participated in the EU-U.S. Privacy Shield Framework and that it Adhered to its Principles

31. The EU-U.S. Privacy Shield framework ("Privacy Shield") was designed by the U.S. Department of Commerce ("Commerce") and the European Commission to provide a mechanism for U.S. companies to transfer personal data outside of the EU that is consistent with the requirements of the European Union Directive on Data Protection. Enacted in 1995, the Directive set forth EU requirements for privacy and the protection of personal data. Among other things, it requires EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission has made a determination that the recipient jurisdiction's laws ensure the protection of such personal data. This determination is referred to commonly as meeting the EU's "adequacy" standard.

32. To satisfy the EU adequacy standard for certain commercial transfers, Commerce and the European Commission negotiated the EU-U.S. Privacy Shield framework, which went into effect in July 2016. The EU-U.S. Privacy Shield framework allows companies to transfer personal data lawfully from the EU to the United States. To join the EU-U.S. Privacy Shield framework, a company must self-certify to Commerce that it complies with the Privacy Shield Principles and related requirements that have been deemed to meet the EU's adequacy standard. Any company that voluntarily withdraws or lets its self-certification lapse must continue to apply the Privacy Shield principles to the personal information it received while a participant in the Privacy Shield and affirm to Commerce on an annual basis its commitment to do so, for as long as it retains such information.

33. Companies under the enforcement jurisdiction of the FTC, as well as the U.S. Department of Transportation, are eligible to join the EU-U.S. Privacy Shield framework. A company under the FTC's jurisdiction that claims it has self-certified to the Privacy Shield Principles, but failed to self-certify to Commerce, may be subject to an enforcement action based on the FTC's deception authority under Section 5 of the FTC Act.

34. Commerce maintains a public website, https://www.privacyshield.gov/welcome, where it posts the names of companies that have self-certified to the EU-U.S. Privacy Shield framework. The listing of companies, https://www.privacyshield.gov/list, indicates whether the company's self-certification is current.

35. On May 11, 2017, Cambridge Analytica joined Privacy Shield. While the Facebook data harvested through the GSRApp predated its participation in Privacy Shield and is therefore not subject to its protections, Cambridge Analytica continued to collect Facebook and other data from or about U.S. and European consumers after it joined Privacy Shield.

36. Until at least November 27, 2018, Cambridge Analytica disseminated or caused to be disseminated privacy policies and statements on https://cambridgeanalytica.org including, but not limited to, the following statements:

> **IS CAMBRIDGE ANALYTICA PART OF THE PRIVACY SHIELD FRAMEWORK?**
>
> Yes: Cambridge Analytica adheres to the EU-US Privacy Shield Principles for the transfer of EU data we use to provide our services, including the onward transfer liability provisions. With respect to personal data received or transferred pursuant to the Privacy Shield Framework, Cambridge Analytica is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. More information on the principles are available at the Privacy Shield website: https://www.privacyshield.gov/.

37. Cambridge Analytica, however, did not complete the steps necessary to renew Cambridge Analytica's participation in Privacy Shield after that certification expired on or about May 11, 2018, nor did they withdraw and affirm their commitment to protect any personal information they had acquired while in the program. After allowing Cambridge Analytica's certification to lapse, Cambridge Analytica continued to claim, as indicated in Paragraph 36, that it participates in Privacy Shield.

VIOLATIONS OF THE FTC ACT

Deceptive Claim Concerning the Collection of Personal Identifiable Information (Count I)

38. Through the means described in Paragraph 23, Cambridge Analytica represented, directly or indirectly, expressly or by implication, that the GSRApp did not collect any identifiable information from Facebook users who authorized the app.

39. In fact, as described in Paragraphs 24-25, the GSRApp collected identifiable information from Facebook users who authorized the App, including the Facebook User ID of those users who used it. Therefore, the representation set forth in Paragraph 38 is false or misleading.

Deceptive Claim by Cambridge Analytica Concerning Participation in Privacy Shield (Count II)

40. As described in Paragraph 36, Cambridge Analytica represented, directly or indirectly, expressly or by implication, that it was a participant in Privacy Shield until at least November 27, 2018.

41. In fact, as described in Paragraph 37, Cambridge Analytica did not renew its participation in Privacy Shield and allowed its certification to lapse in May 2018. Therefore, the representation set forth in Paragraph 40 is false or misleading.

Deceptive Claim by Cambridge Analytica Concerning Compliance with Continuing Obligations in Privacy Shield (Count III)

42. As described in Paragraph 36, Cambridge Analytica represented that Cambridge Analytica adheres to the Privacy Shield principles. These principles include a requirement that if a company ceases to participate in Privacy Shield, it must affirm to Commerce that it will continue to apply the principles to personal information that it received during the time it participated in the program.

43. In fact, as described in Paragraph 37, Cambridge Analytica has not affirmed to Commerce that they will continue to apply the principles to personal information that Cambridge Analytica received during the time Cambridge Analytica participated in the program. Therefore, the representation set forth in Paragraph 42 is false or misleading.

NOTICE

You are notified that on March 24, 2020, at 10:00 a.m., at the Federal Trade Commission offices, 600 Pennsylvania Avenue, NW, Room 532-H, Washington, D.C. 20580, an Administrative Law Judge of the Federal Trade Commission, will hold a hearing on the charges set forth in this Complaint. At that time and place, you will have the right under the Federal Trade Commission Act to appear and show cause why an order should not be entered requiring you to cease and desist from the violations of law charged in this Complaint.

You are notified that you are afforded the opportunity to file with the Federal Trade Commission ("Commission") an answer to this Complaint on or before the 14th day after service of the Complaint upon you. An answer in which the allegations of the Complaint are contested must contain a concise statement of the facts constituting each ground of defense; and specific admission, denial, or explanation of each fact alleged in the Complaint or, if you are without knowledge thereof, a statement to that effect. Allegations of the Complaint not thus answered will be deemed to have been admitted.

If you elect not to contest the allegations of fact set forth in the Complaint, the answer should consist of a statement that you admit all of the material facts to be true. Such an answer will constitute a waiver of hearings as to the facts alleged in the Complaint and, together with the Complaint, will provide a record basis on which the Commission may issue a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding. In such answer, you may, however, reserve the right to submit proposed findings of fact and conclusions of law under FTC Rule § 3.46.

Failure to answer timely will be deemed to constitute a waiver of your right to appear and contest the allegations of the Complaint. It will also authorize the Commission, without further

notice to you, to find the facts to be as alleged in the Complaint and to enter a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding.

The Administrative Law Judge will hold an initial prehearing scheduling conference to be held not later than 10 days after the answer is filed by the Respondent. Unless otherwise directed by the Administrative Law Judge, the scheduling conference and further proceedings will take place at the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Room 532-H, Washington, D.C. 20580. Rule 3.21(a) requires a meeting of the parties' counsel as early as practicable before the prehearing scheduling conference, but in any event no later than 5 days after the answer is filed by the Respondent. Rule 3.31(b) obligates counsel for each party, within 5 days of receiving a Respondent's answer, to make certain initial disclosures without awaiting a formal discovery request.

The following is the form of the order which the Commission has reason to believe should issue if the facts are found to be as alleged in the Complaint. If, however, the Commission concludes from record facts developed in any adjudicative proceedings in this matter that the proposed order provisions as to Respondent[s] might be inadequate to fully protect the consuming public, the Commission may order such other relief as it finds necessary and appropriate.

Moreover, the Commission has reason to believe that, if the facts are found as alleged in the Complaint, it may be necessary and appropriate for the Commission to seek relief to redress injury to consumers[, or other persons, partnerships or corporations. Such relief could be in the form of restitution for past, present, and future consumers and such other types of relief as are set forth in Section 19(b) of the Federal Trade Commission Act. The Commission will determine whether to apply to a court for such relief on the basis of the adjudicative proceedings in this matter and such other factors as are relevant to consider the necessity and appropriateness of such action.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. "Covered Information" means the following information from or about an individual consumer including: (a) a first and last name; (b) a physical address or precise geolocation; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license or other government-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a "cookie," a mobile device ID, or processor serial number; (j) data fields that can be accessed or collected through Facebook from or about Facebook Users or their Friends (*e.g.*, "likes," "hometowns," "birthdates," "photos," "gender," "educational information," "religious or political views," or "marital" or other "relationship" status); (k) information that is created,

maintained, or accessed by the consumer (*e.g.*, "messages"); (l) any data regarding a consumer's activities online (*e.g.*, searches conducted, web pages visited, or content viewed); or (m) any user credentials, such as a username and password.

B. "Facebook" means Facebook Inc., its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, members, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

C. "GSRApp" means all iterations of the GSRApp Facebook application that first began operating on the Facebook platform in May 2014.

D. "Respondent" means Cambridge Analytica, LLC, and its successors and assigns.

E. "Trustee" means Salvatore Lamonica, Esq., appointed Chapter 7 Trustee for Respondent in the United States Bankruptcy Court for the Southern District of New York, Case No. 19-11500 (SHL).

Provisions

I. Prohibition against Misrepresentations about Covered Information

IT IS ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service must not misrepresent in any manner, expressly or by implication, the extent to which they protect the privacy and confidentiality of any Covered Information, including:

A. The extent to which they collect, use, share, or sell any Covered Information; and

B. The purposes for which they collect, use, share, or sell any Covered Information.

II. Prohibition against Misrepresentations about Participating in Privacy or Security Programs

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service must not misrepresent in any manner, expressly or by implication, the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

III. Requirement to Meet Continuing Obligations Under Privacy Shield

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service shall not possess or control personal information from European Union residents that Respondent received while it participated in the EU-U.S. Privacy Shield framework, unless Respondent:

A. affirms to the Department of Commerce, within ten (10) days after the effective date of this Order and on an annual basis thereafter for as long as it retains such information, that it will:

    1. continue to apply the EU-U.S. Privacy Shield framework principles to the personal information it received while it participated in the Privacy Shield; or

    2. protect the information by another means authorized under EU (for the EU-U.S. Privacy Shield framework) or Swiss (for the Swiss-U.S. Privacy Shield framework) law, including by using a binding corporate rule or a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the European Commission; or

For purposes of this subprovision, Respondent does not possess or control personal information in the possession of a government regulatory or law enforcement agency, including the United Kingdom's Information Commissioner's Office.

B. returns or deletes the information within ten (10) days after the effective date of this Order; or if, as of the effective date of this Order, the information is in the possession of a government regulatory or law enforcement agency, including the United Kingdom's Information Commissioner's Office, returns or deletes the information within ten (10) days after the information is returned to Respondent.

IV. Required Deletion of Data

IT IS FURTHER ORDERED that Respondent, and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must:

A. Provide, within ten (10) days from the effective date of this Order, the Commission with a written statement, sworn under penalty of perjury, providing the name, address, and phone number for each person with whom Respondent shared any Covered Information collected from consumers through GSRApp, and any information that originated, in whole or in part, from this Covered Information;

B. Delete or destroy all Covered Information collected from consumers through GSRApp, and any information or work product, including any algorithms or

equations, that originated, in whole or in part, from this Covered Information. Such deletion or destruction must occur within ten (10) days of the effective date of this Order, or if such information is in the possession of a government regulatory or law enforcement agency, including the United Kingdom's Information Commissioner's Office, as of the effective date of this Order, within ten (10) days after the Covered Information is returned to Respondent. Provided, however, that such Covered Information, or any information that originated in whole or in part from such Covered Information, need not be deleted or destroyed for so long as requested by a government agency or otherwise required by regulation, court order or other legal obligation; and

C. Provide a written statement to the Commission, sworn under penalty of perjury, confirming the foregoing. This statement must be provided: (1) within thirty (30) days after the effective date of the Order; or, if applicable, (2) within thirty (30) days after the Covered Information is returned to Respondent from a government regulatory or law enforcement agency, or within thirty (30) days after any legal obligation to preserve the Covered Information has ended.

V. Duty to Protect Covered Information

IT IS FURTHER ORDERED that Respondent, and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, are permanently restrained and enjoined from disclosing, using, selling, or receiving any benefit from Covered Information or any information that originated, in whole or in part, from this Covered Information.

VI. Access to Corporate Documents and Data

IT IS FURTHER ORDERED that the Trustee shall make available to the Commission, for inventory and copying, all correspondence, email, financial data including tax returns, and any other documents, computer equipment, and electronically stored information, in Trustee's possession, custody, or control, that contain information about Respondent's role and assets at the Commission's expense. The Commission shall return each item produced for inventory or copying to the Trustee within ten (10) business days from the data and time of the Trustee's delivery of each such item.

IT IS FURTHER ORDERED that the Trustee, to the extent he has possession, custody, or control of computer equipment or electronically stored information described above, shall provide the Commission with any necessary means of access to the computer equipment or electronically stored information, including, but not limited to, computer access codes and passwords.

IT IS FURTHER ORDERD that the Trustee shall provide notice to the Commission of the proposed abandonment of any corporate books or records of Respondent, and upon the Commission's designation, the Trustee shall transfer such books and records to the Commission.

VII. Order Effective Dates

IT IS FURTHER ORDERED that the final and effective date of this Order is the 60th day after this Order is served. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than twenty (20) years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

THEREFORE, the Federal Trade Commission, this twenty-second day of July, 2019, has issued this Complaint against Respondent Cambridge Analytica.

By the Commission.

April J. Tabor
Acting Secretary

SEAL: