

BY EMAIL <media@socialscience.one>¹

July 12, 2018

Professor Gary King
Professor Nathaniel Persily
Social Science One

Dear Professor King and Professor Persily,

We write to you, as co-chairs of Social Science One, to urge you to immediately suspend the data analysis activities announced this week,² pending a thorough and independent investigation of the privacy protections for Facebook users. For multiple reasons set out below, including the fact that the program does not comply with the GDPR and violates Facebook's 2011 consent order with the Federal Trade Commission, we do not believe the project may go forward.

While we respect the efforts to develop a new model for industry-academic partnerships, frankly you could not have picked a more controversial data set to launch this initiative. The third-party use of Facebook data has been the focus of substantial Congressional hearings, hearings in the European Parliament, and an extensive inquiry in the UK.³ The recent report of the UK Information Commissioner's Office had this to say about the transfer of Facebook user data to research institutions: "Based on evidence we have in our possession, we are concerned about the way in which data was accessed from the Facebook platform and used for purposes it was not intended for or that data subjects would not have reasonably expected."⁴ We recognize the opportunity provided by new privacy-preserving techniques to permit research access to very large data sets,⁵ but again you have chosen the most controversial data set to test these methods.

¹ It is notable that no contact information is provided for any individual at the Social Science One website, nor is there any indication that a person has been designated by Social Science One to assess the privacy ramifications of the project.

² Social Science One, *Independent Research Commission Partnering with Facebook and 7 Nonprofit Foundations to Study Role of Social Media in Elections and Democracy Reveals New Name and Announces First Data Set is Available for Academic Research* (July 11, 2018), <https://socialscience.one/blog/social-science-one-public-launch>

³ EPIC, *In re Facebook (Cambridge Analytica)*, <https://epic.org/privacy/facebook/cambridge-analytica/>.

⁴ Information Commissioner's Office, *Investigation Into the Use of Data Analytics In Political Campaigns*, (Jul. 10, 2018) at 22, <https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>.

⁵ See National Academies of Sciences, Engineering, and Medicine; Division of Behavioral and Social Sciences and Education; Committee on National Statistics; *Panel on Improving Federal Statistics for Policy and Social Science Research Using Multiple Data Sources and State-of-the-Art Estimation Methods*; Harris-Kojetin BA, Groves RM, editors. Federal Statistics, Multiple Data Sources, and Privacy Protection: Next Steps. Washington (DC): National Academies Press (US); 2017 Oct 2. Available from: <https://www.ncbi.nlm.nih.gov/books/NBK475779/> doi: 10.17226/24893

Social Science One describes the Facebook data as “the largest and most comprehensive information base ever used to study social media, and even some of the most extensive data ever used to study human behavior in general.”⁶ It is therefore of the utmost importance that you abide by all legal and ethical obligations related to the privacy rights of Facebook users.

I. Facebook Users Have Not Provided Meaningful Consent for the Collection and Use of Their Data

EPIC fully supports academic research on the effects of social media on democracy and elections. In fact, EPIC launched a project a year ago dedicated to safeguarding democratic institutions from foreign interference.⁷ EPIC is presently engaged in several matters seeking information about Russian interference in the 2016 U.S. presidential election.⁸ It is ironic and deeply troubling, however, that this research project involves violating the privacy of Facebook users’ for the purpose of learning how social media influences elections. It was this very type of massive data collection by political firms such as Cambridge Analytica that raised alarms about the influence of social media on elections in the first place. In fact, the data obtained by Cambridge Analytica was originally collected for the purpose of academic research.

That is why the lack of meaningful consent from users necessitates suspending this study. Informed consent of human subjects is a basic ethical obligation for researchers, but one that Facebook and Social Science One have ignored. Facebook users will have no say over whether their personal data is used for this study. Facebook will not provide user with any mechanism to affirmatively opt-in to the use of their data. Neither Facebook nor Social Science One have indicated that Facebook users will even be provided with any information regarding the use of their data for this study. There is no indication that Facebook users will have the ability to opt-out if they do not wish to have their data used for research purposes. Facebook states that “[f]undamental to this entire effort is ensuring that people’s information is secure and kept private.”⁹ But Facebook cannot claim to be respecting the privacy of its users if it fails to give users any control over whether their personal data is collected and used for this study.

II. The Transfer of Data Violates the FTC’s 2011 Consent Order with Facebook

⁶ <https://socialscience.one/our-facebook-partnership>

⁷ EPIC, DEMOCRACY AND CYBERSECURITY: PRESERVING DEMOCRATIC INSTITUTIONS, <https://www.epic.org/democracy/>.

⁸ See, EPIC v. FBI, <https://www.epic.org/foia/fbi/russian-hacking/> (seeking records related to the FBI's response to foreign cyber attacks on democratic institutions in the United States prior to the 2016 Presidential Election); EPIC v. ODNI, <https://www.epic.org/foia/odni/russian-hacking/> (seeking release of the Complete ODNI Assessment of the Russian interference with 2016 U.S. Presidential Election).

⁹ Elliot Schrage and David Ginsberg, *Facebook Launches New Initiative to Help Scholars Assess Social Media’s Impact on Elections*, Facebook Newsroom (Apr. 9, 2018), <https://newsroom.fb.com/news/2018/04/new-elections-initiative/>.

The FTC's 2011 Consent Order with Facebook is clear: Facebook must obtain affirmative express consent before disclosing personal information to third parties.¹⁰ The Consent Order states that Facebook shall, prior to disclosing any information to third parties beyond the restrictions imposed by the user's privacy settings:

Clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and **obtain the user's express consent.**¹¹

As the FTC explained, this is a requirement that Facebook "obtain consumers' affirmative express consent before enacting changes that override their privacy preferences."¹² It is not enough for Facebook to bury a notice in its privacy policy – in addition to obtaining a user's affirmative consent Facebook must provide users with a clear and prominent disclosure that includes the identity of the third parties to whom the personal information will be transferred.

By transferring personal information to third-party researchers without (1) providing clear and prominent notice and (2) obtaining the affirmative express consent of users, Facebook will in clear violation of the 2011 Consent Order with the FTC. The *Wall Street Journal* has reported that outside researchers will have "the same access that employees would have" to user data.

The 2011 Consent Order was the result of Facebook's significant privacy violations, which EPIC documented in detailed complaints to the FTC in 2009 and 2010.¹³ Chief among them was Facebook's practice of making non-public information available to third parties without users' knowledge or consent.¹⁴ As we stated in 2009:

Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available.¹⁵

Earlier this year, Facebook was found to have allowed the political data mining firm Cambridge Analytica to obtain the personal information on 87 million users, prompting inquiries from U.S. and international lawmakers. As EPIC told Congress, "Facebook's admission that it

¹⁰ Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>.

¹¹ *Id.*

¹² Fed. Trade Comm'n., *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, Press Release (Nov. 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

¹³ See, *In the Matter of Facebook, Inc.* (EPIC, Complaint, Request for Investigation, Injunction, and Other Relief) before the Federal Trade Commission, Washington, D.C. (filed Dec. 17, 2009), <http://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf>.

¹⁴ *Id.*

¹⁵ *Id.*

disclosed data to third parties without users' consent suggests a clear violation of the 2011 Facebook Order."¹⁶ The U.K. Information Commissioner's Office recently fined Facebook the maximum allowable fine under U.K. law as the result of this data transfer, charging Facebook with "failing to safeguard people's information [and] failing to be transparent about how people's data was harvested by others and why they might be targeted by a political party or campaign."¹⁷ The FTC has recently announced that it is investigating Facebook.¹⁸ As the Acting Director of the Bureau of Consumer Protection stated:

The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against companies that fail to honor their privacy promises, including to comply with Privacy Shield, or that engage in unfair acts that cause substantial injury to consumers in violation of the FTC Act. Companies who have settled previous FTC actions must also comply with FTC order provisions imposing privacy and data security requirements. Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices.¹⁹

Many State Attorneys General have also announced their investigations into the matter.²⁰

Given Facebook's obligations under the FTC Consent Order and its continuing violations of user privacy, it is particularly troubling that you plan to move forward with plans to collect the data of 2.2 billion Facebook users without their consent. This proposal not only violates the FTC Consent Order, but the privacy rights of Facebook's 2.2 billion users.

The Social Science One study should be suspended pending a determination by the FTC regarding Facebook's compliance with the 2011 Consent Order.

III. Facebook's Prior Relations with Researchers Have Raised Significant Questions

Facebook has a sordid history of privacy violations when doing research, and Social Science One is inadequately prepared to protect the privacy of its research subjects. Social Science One represents that "All research projects must pass the standard peer-review protocols of academic social science, with the addition of a special ethical review designed for the unique challenges of

¹⁶ Letter from EPIC to S. Comm on the Judiciary, (Apr. 9, 2018), <https://epic.org/testimony/congress/EPIC-SJC-Facebook-Apr2018.pdf>.

¹⁷ Information Commissioner's Office, *Investigation Into the Use of Data Analytics In Political Campaigns*, (Jul. 10, 2018), <https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>.

¹⁸ Fed. Trade Comm'n., *Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices* (Mar. 26, 2018), <https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection>.

¹⁹ *Id.*

²⁰ See, EPIC, *State AGs Launch Facebook Investigation*, (Mar. 26, 2018), <https://epic.org/2018/03/state-ags-launch-facebook-inve.html>.

analyzing the types of questions and data.”²¹ As you are aware, Cambridge Analytica was able to exploit data because Facebook gave improper access to an academic researcher. Therefore, the fact that this research will be subject to standard peer-review protocols and Facebook’s ethical review methods—as research using Facebook data has been subject to in the past—does not sufficiently address the privacy risks.

Facebook’s record with researchers indicates a disregard for user privacy and consent. In 2012, Facebook conducted an experiment that secretly manipulated user emotions by seeing if exposing users to more positive or negative content in their News Feed would affect their posting behaviors.²² This was done by running randomized A/B testing on Facebook’s platform, and Social Science One has stated that it is considering using data from randomized A/B tests run on Facebook’s platform in the future.²³ Social Science One has not adequately addressed the ethical mistakes Facebook has made in the past and indicated how it will conduct its research differently.

IV. Voting data are extremely sensitive

Data on an individual’s political views and voting habits are among the most sensitive types of personal information. Social Science One plans to combine post-election surveys (from Mexico, Brazil, Sweden, United States, and India) with Facebook data to research the effect of social media on elections.²⁴ Anonymity is a fundamental aspect of voting rights in the U.S. and in many other countries. Matching data on how people voted with their detailed Facebook profiles threaten to undermine that fundamental right.

The public cares deeply about the confidentiality of their voting data. Last year the Presidential Election Commission sought to wrongfully obtain voter data from all 50 states for the alleged purpose of investigating voter fraud. There was a public outcry, and many states refused to turn over their voter rolls to the federal government. EPIC (and several other groups) sued the Commission because its collection of the personal data of millions of registered voters was an unconstitutional invasion of privacy and its failure to conduct a Privacy Impact Assessment violated the E-Government Act.²⁵ The Commission was disbanded following the public opposition and lawsuits.²⁶

V. Violation of GDPR

The General Data Protection Regulation (“GDPR”) applies to the processing of personal data that monitors the behavior of individuals within the European Union. The heightened requirements of the GDPR will apply to the research proposed by Social Science One, even if the processing occurs in the US.

²¹ <https://socialscience.one/overview>

²² EPIC, *In re Facebook (Psychological Study)*, <https://www.epic.org/privacy/internet/ftc/facebook/psycho/>.

²³ <https://socialscience.one/future-datasets>

²⁴ <https://socialscience.one/future-datasets>.

²⁵ *EPIC v. Commission*, <https://epic.org/privacy/litigation/voter/epic-v-commission/>.

²⁶ Executive Order 13820 (Jan. 3, 2018), <https://epic.org/privacy/litigation/voter/epic-v-commission/EPIC-v-Commission-termination-exec-order-010318.pdf>.

In particular, Article 9 of the GDPR stipulates that “processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.” The profiles of 2.2 billion Facebook users encompass virtually all of these sensitive data categories, which require the strictest safeguards for processing under the GDPR, even for academic research purposes.

The scope and purposes of the research proposed by Social Science One fail to meet the exemption for the processing of special categories of personal data on academic research grounds.

Article 89(1) of the GDPR requires that “processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner...”

Article 9(2)(j) of the GDPR requires that the extent of processing sensitive data for the purposes of academic research shall only be allowed if adheres to Article 89(1) and is “proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.”

The emphasis lies on data minimization foremost, then strict pseudonymization. Social Science One’s access to 2.2 billion Facebook users’ data in no way demonstrates either safeguard to meet the requirements of the GDPR. Due to the immensity and granularity of data disclosed by Facebook, the purposes of safeguarding the fundamental rights and interests of the data subject can no longer be achieved by pseudonymization, or “de-identification.”

First, the sheer extent of data available to Social Science One violates a fundamental tenet of the GDPR—data minimization (Article 5). The research groups have not taken any active steps to implement technical and organizational measures to limit the processing of sensitive data. By accepting access to this massive trove of sensitive personal information, the groups have also failed to adequately assess the risks to the rights and freedoms of individuals as per GDPR Recital 75, and violated the rights to information about processing and access to data for individuals (Articles 13 and 15). There remain significant risks for the unauthorized reversal of pseudonymization with catastrophic effects on the privacy of individuals. This already constitutes multiple violations of the GDPR.

Secondly, reports that the researchers will share access to Facebook’s proprietary user data indicate that Social Science One has no technical or organizational measures in place to pseudonymize data to the standard required by the GDPR. Recital 29 requires “additional information for attributing the personal data to a specific data subject [to be] kept separately.” The groups have not implemented this, as evidenced by today’s Wall Street Journal report: “to determine which data sets to release, a half-dozen primary researchers will have broad access to Facebook’s proprietary user data, said Gary King, a social science professor at Harvard University and one of the co-chairs of the research group.”

Furthermore, Article 29 Working Party’s Opinion 05/2014 on Anonymisation Techniques established that de-identification must be “irreversible.” This is a higher bar than simply removing personally identifiable information such as names and birthdays from perhaps the most comprehensive dataset ever compiled. Therefore, this proposed study violates EU data protection laws and irresponsibly imperils the privacy rights of individuals.

Conclusion

This research initiative violates U.S. and European law. Social Science One should suspend its research until the FTC is able to complete a full investigation. You say that you intend to conduct this research “according to the highest standards of data privacy”²⁷ but there is not even a designated privacy official to help make this determination.

The concerns that EPIC has outlined in this letter are widely shared. We urge you to consider carefully the consequences of the misuse of personal data that may result from this undertaking.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Christine Bannan
Christine Bannan
EPIC Administrative Law and Policy Fellow

/s/ Sunny Kang
Sunny Kang
EPIC International Consumer Counsel

/s/ Sam Lester
Sam Lester
EPIC Consumer Privacy Fellow

Cc: Commissioners of the US Federal Trade Commission
Chair of the European Union Data Protection Board

²⁷ <https://socialscience.one/our-facebook-partnership>