March 29, 2018

Dear Member of Congress,

We write to thank you for your attention to the revelations regarding Cambridge Analytica, a UK-based subsidiary of SCL Group, and its relationship with Facebook, which raise new questions about Facebook's commitment to user privacy.

We encourage you to seek out answers from both companies about how and why the sensitive personal data of millions of people were transmitted to Cambridge Analytica, how the company allegedly kept this information for several years, and what it was used for. Further, we call on you to hold hearings on the private-sector practice of overbroad collection and exploitation of sensitive personal information and the urgent need for data protection legislation to protect user rights.

Background

In 2014, a group of social scientists led by Aleksandr Kogan created and deployed a personality test via a Facebook app. The app gave researchers access to detailed personal information not only about the individuals who used the app, but also all of their Facebook friends. These friends had no contact with the app and therefore could not have consented to the use of their data. Reports indicate that up to 50 million people could have had their data mined by Kogan.

Global Science Research (GSR), Kogan's company, contracted to disclose the data he collected to Cambridge Analytica, which had invested in advertising and promoting the app to increase the number of users it reached (some users were even paid to authorize the app). Cambridge Analytica manipulated the data to, among other things, create and purchase highly targeted ads that were used to influence the 2016 U.S. presidential elections, as well as potentially for other high-profile elections and debates.[1] Facebook has claimed that, after learning that GSR transmitted user data to Cambridge Analytica, it demanded the data be deleted, though it appears the company did not adequately ensure the deletion happened.[2]

This transaction was not a data breach, nor a hack, but instead the foreseeable consequence of a common business model: the widespread (over) collection and processing of personal information to create Facebook users profiles, in particular to generate better ad targeting. Overcollection of user information is common practice, as is the practice of distributing that information to a large number of third-party companies, many of which are not known to the

[1] http://uk.businessinsider.com/cambridge-analytica-has-contradicted-itself-on-its-work-for-leaveeu-2018-3?r=UK&IR=T. In 2015, after but not necessarily related to this incident, Facebook changed its rules to prohibit app developers from accessing the personal information of friends of app users. https://techcrunch.com/2015/04/28/facebook-api-shut-down/.

[2] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

users.[3] During these transactions, the only governing instrument is often a company's broad and inaccessible terms of service, just as it was with the collection of Facebook data by GSR. This means there is little to no transparency for users to understand the full scope of a company's data practices, not to mention the practices of third parties like Cambridge Analytica, which never have direct interaction with users. Typically, users have limited capacity to control the access that app developers have to their information, limited capacity to ask for that information to be deleted, and no notice when their information has been transferred to third parties.

Facebook, GSR, and Cambridge Analytica

It is critical that representatives from Facebook, GSR, and Cambridge Analytica answer questions about the events and circumstances that led to the personal information of 50 million users moving between the organizations:

1. Was Facebook able to determine that Cambridge Analytica was using data that Facebook says it ordered deleted for micro-targeted ad campaigns? If so, when was the company able to make that determination?
2. At what level at Facebook did staff make the decision not to notify users that GSR abused their data?
3. Did Cambridge Analytica receive information of non-U.S. citizens as well as people in the United States? If so, is there a legal justification under domestic laws, like those of the European Union, to justify that disclosure?
4. Does Facebook have evidence that other app providers have or are now engaging in practices similar to GSR and Aleksandr Kogan? If so, approximately how many app providers does Facebook believe to have abused user data, and what has Facebook done in response?
5. Was the incident with GSR and Cambridge Analytica reported in the independent audits that Facebook is required to obtain under its consent order with the Federal Trade Commission? What, if any, remedy was recommended?
6. How was the relationship between Aleksandr Kogan and Cambridge Analytica formed, and what, if any, influence did Cambridge Analytica have on the development of the app? Specifically, when did GSR and Cambridge Analytica enter into a contract regarding the acquisition of user data and what were the terms of that contract?
7. Has Cambridge Analytica worked with any other app provider to receive user data?
8. Has GSR or Aleksandr Kogan contracted with any other company regarding user data?
9. Has Cambridge Analytica now deleted all of the personal data it received from GSR, Aleksandr Kogan, or any other app provider? How did Cambridge Analytica analyze that data and what information were they able to derive from the raw data that they received from Facebook? Has that derivative information also been deleted? If not, where and how is Cambridge Analytica using that data?

[3] https://rebecca-ricks.com/paypal-data/.

10. Has Facebook considered limiting data collection or giving users other more granular control options over the information that it collects in order to provide more transparency to users and help protect against future abuse?

Moving Toward Solutions

Protecting personal data means establishing clear rules that any entity that processes your information must follow. In less than three months, Europe's General Data Protection Regulation will enter full force, providing perhaps the most comprehensive data protection framework in the world. Countries including Tunisia, Japan, Argentina, Australia, Jamaica are also considering new data protection laws or upgrading their frameworks. An expert committee in India is currently deliberating on a data protection and privacy regime for the next billion users of the internet.[4] The committee was formed in the backdrop of important privacy and data protection cases that are being heard before a constitutional bench of the Supreme Court of India, on India's national identity program, "Aadhaar" and the legality of transferring users' data between WhatsApp and Facebook.[5]

Notably missing from the list of countries creating a federal framework for data protection is the U.S., where many leading technology companies are headquartered.[6] Traditionally the Federal Trade Commission has played a role in this area, though while individual Commissioners have taken strong approaches, the role of the agency overall is limited and their commitment to enforcing their consent orders has been questioned. This means that, as the global tide continues to shift and users demand more transparency and redress, the U.S. continues to lag behind, with regulators claiming that protecting users will impede "innovation," while companies cling to abusive business models that are built on the stockpiling and manipulation of personal data.

Today, it has become increasingly clear that these models are broken. It is critical that the U.S. moves beyond a piecemeal, industry-specific approach, not only to protect people but also to provide stability to the industry and promote competition. This means that legislation is needed to incentivize alternative business models, prevent data misuse and abuse, provide greater transparency, and to give people avenues for redress when their rights are violated. We urge you to consider developing a framework to give companies substantive rules, including rules to govern the collection and use of these data, to give users the capacity to delete their data or remove it from a platform, and to provide transparency for third-party sharing.

---

[4] http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited.
[5]https://www.bloombergquint.com/aadhaar/2018/03/21/the-key-arguments-in-supreme-court-against-aadhaar; https://scroll.in/latest/844688/centre-tells-supreme-court-it-will-frame-regulations-to-protect-user-data.
[6] Despite never having passed a data protection law, the US has played a pivotal role in data protection, having developed the "fair information practices" that have influenced modern data protection laws.

Access Now created the attached guide to help lawmakers considering data protection frameworks. We hope you find it useful, and we are available to answer any other questions you may have.

Thank you for your work on this important issue.

Sincerely,

Amie Stepanovich
U.S. Policy Manager

Nathan White
Senior Legislative Manager