RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS

United States Senate

WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-9673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958

915 LAFAYETTE BOULEVARD, SUITE 304
BRIDGEPORT, CT 06604
(203) 330-0598
FAX: (203) 330-0608

http://blumenthal.senate.gov

April 19, 2018

The Honorable Maureen Ohlhausen
Acting Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Acting Chairman Ohlhausen,

I am pleased that the Federal Trade Commission (FTC) has opened an investigation into the privacy practices and policies at Facebook. Recent revelations about the illegitimate harvesting of personal data on tens of millions of Americans have shed new light on the systemic failure of Facebook to address privacy risks and keep its promises to users. Despite Mark Zuckerberg's recent apology tour, Facebook's history of negligence demonstrates that the company can no longer be trusted to self-regulate. I write to draw attention to information that may be relevant to your investigation, including evidence that Facebook may have violated its consent decree. I also encourage the FTC to pursue strong legal remedies to compensate consumers harmed and set enforceable rules on its future conduct.

In November 2011, Facebook agreed to a proposed settlement containing a consent decree after the FTC found that the company had deceived consumers by sharing personal data with advertisers and making public information previously designated as private. Under the settlement, Facebook was barred from misrepresenting the privacy of personal information and was required to obtain affirmative express consent before enacting changes would override privacy preferences. The FTC also required Facebook to establish "a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information."

Facebook's adherence to the consent decree has been called into question based on recent reports that the political consulting firm Cambridge Analytica and Global Science Research (GSR) had harvested a large-scale dataset of Facebook users based on a third-party app. The GSR app would collect demographic details, private communications, and other profile metrics of those who installed the app and their friends. Based on Facebook's permissive, default privacy settings, Cambridge Analytica was able to obtain information from up to 87 million profiles based on only about 300,000 users installing the GSR app.

This should have never happened. The FTC put Facebook on notice about the privacy risks of third-party apps in its complaint. Three of the FTC's claims concerned the misrepresentation of verification and privacy preferences of third-party apps. In 2008, shortly after the launch of its developer platform, Facebook introduced a "Verified Apps" program, which would provide a badge that Facebook had certified the security, privacy, trustworthiness, and transparency of an app.[1] When Facebook announced it would be ending the program the following year, it claimed that it would be extending these trust standards into *all* apps. However, in its 2011 complaint, the FTC found that despite claims of auditing, Facebook took no steps to verify either the security or protections for collected user information. Seven years later, exactly how Facebook verifies third-party apps is still murky.

The Cambridge Analytica revelations demonstrate that Facebook continued to turn a blind eye to third-party apps despite the FTC mandated privacy program. Facebook should have been aware that GSR was planning to violate developer platform rules based on the policies that developers are required to submit. GSR's terms of service ("Attachment 1") stated explicitly that it reserved the right to sell user data and would collect profile information from friends. These terms of service should have put Facebook on notice that GSR may be seeking to sell user data. At this month's Senate hearing on Facebook, Mr. Zuckerberg informed me that its app review team would have been responsible for vetting the policy and acknowledged that Facebook "should have been aware that this application developer submitted a [terms of service] that was in conflict with the rules of the platform."

Even the most rudimentary oversight would have uncovered these problematic terms of service. Moreover, Facebook knew as early as 2010 that third-party app developers were selling information to data brokers.[2] The fact that Facebook did not uncover these non-compliant terms strongly suggests that its "comprehensive privacy program" established pursuant to the FTC consent decree was either inadequate to address threats or not followed in practice. This willful blindness left users vulnerable to the actions of Cambridge Analytica.

The Cambridge Analytica matter also calls into question Facebook's compliance with the consent decree's requirements to respect privacy settings and protect private information. Three years after Facebook agreed to the consent decree, Facebook by default continued to provide broad access to personal data to third party apps, data that may not have been marked as public. In evaluating claims of deception and misrepresentation of privacy controls, the FTC has typically considered what a consumer would have reasonably understood their settings to mean. No information was readily provided to users about this permissive sharing to third-party apps or how to opt out. Nor were users informed about which apps accessed their profiles or given the ability to resolve unwanted intrusions. While users could be judicious about their privacy settings and the apps they installed, the actions of only one friend could thwart their efforts without their knowledge. The ease with which the GSR app was able to harvest data on 87 million users

---

[1] "Guiding Principles." Facebook Developers.
https://web.archive.org/web/20080902015608/http://developers.facebook.com/get_started.php?tab=principles

[2] "Facebook Shuts Down Apps That Sold User Data, Bans Rapleaf." AdAge. October 29, 2010.
www.adweek.com/digital/facebook-shuts-down-apps-that-sold-user-data-bans-rapleaf/

demonstrates that third parties were effectively able to override privacy preferences without express consent.

It is also noteworthy that the relaxation of data retention policies for third party developers may have contributed to the illegitimate collection of data. In a version of its Developer Principles and Policies dated December 1, 2009, Facebook mandated that developers "must not store or cache any data you receive from us for more than 24 hours" and "must not give data you receive from us to any third party."[3] In April 2010, Facebook changed this policy to permit developers to keep user information with significantly reduced restrictions on the sharing of data.[4] There is no indication that Facebook informed its users that third parties would now be allowed to store their data or share it.

Facebook had multiple opportunities to prevent this harvesting and notify users before March 2018, but failed to do so. According to former Cambridge Analytica employee Christopher Wylie, the GSR app had collected data so aggressively that it triggered Facebook's security protocols.[5] However, there is no indication Facebook took steps to investigate or limit the collection despite the problematic terms of service.

Facebook finally acted on the GSR app after *The Guardian* reported on Cambridge Analytica's plans in December 2015. While Facebook removed the application and contacted both companies to request the destruction of user information, its response continued to be inadequate. Facebook did not take any steps to prevent Cambridge Analytica and its partners from continuing to use its platform for advertising or analytics services, even working alongside the company within campaigns. It did not provide notice to users about how their information has been harvested by Cambridge Analytica, nor did it inform the FTC about the collection of data without user consent. Facebook did not contact Christopher Wylie to request the deletion of user data until the following August – at least nine months after the initial report. Facebook took no further action to assess whether data had been deleted. The ineffective response calls into question how seriously the company took this incident and others like it.

Former Facebook employees have told me that its staff were not empowered to effectively enforce privacy policies. For example, Sandy Parakilas, who led efforts to fix privacy problems on its developer platform from June 2011 to August 2012, describes Facebook as a company that would not commit resources or attention to protecting users against violations from third-party apps. Mr. Parakilas' letter to me ("Attachment 2") along with his November 19, 2017 *New York Times* op-ed and April 10, 2018 interview with *New York Magazine*, highlight a deeply disturbing pattern of disregard by Facebook to the privacy risks posed by third-party apps. Mr. Parakilas recounts how one executive told him, after proposing a deeper audit of

---

[3] "Developer Principles and Policies." Facebook Developers. December 1, 2009. https://web.archive.org/web/20091223051700/http://developers.facebook.com/policy/

[4] "A New Data Model." Facebook. April 21, 2010. https://web.archive.org/web/20120502125823/http://developers.facebook.com/blog/post/378/

[5] Cadwalladr, Carole. "'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower." The Observer. March 17, 2018. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

developers' use of data, "Do you really want to see what you'll find?" Had Facebook taken such requests more seriously at the time, the GSR app might have been caught earlier.

Facebook has acknowledged it has neglected its privacy controls, which had non-functional settings and often outdated descriptions did not reflect how the platform operates.[6] Overall Facebook's privacy controls were arcane and difficult to navigate, preventing users from effectuating their preferences. Such deficiencies indicate that Facebook did not maintain an adequate privacy program that was sufficient to protect users and enable them to exercise informed consent.

We may never know the full extent of the damage caused by the failure to provide adequate controls and protection to users. A month after the recent Cambridge Analytica reports, Facebook has not disclosed information on how many applications engaged in similar data collection, but has stated that it expects to have to audit thousands of suspicious applications. As before, it remains only externally reactive to public reports, for example suspending the company CubeYou after media covered its commercial activities. The Facebook developer platform was launched in 2007 and stronger protections for consumers were not implemented until 2015. Presumably many of those companies that developed platform application have shut down, contact details changed, and record trails lost. While Mr. Zuckerberg has committed to audit suspicious apps, it is clear that Facebook will never be able to fully assess the impact of its years of neglect.

Facebook now bears little resemblance to the company it was at the time of the consent decree, necessitating a vigorous investigation into its privacy practices across its range of products and activities. Since November 2011, its expansion and acquisitions have strengthened the company's dominance in the social networking market and increased the significance of the challenges posed to consumers. Consumers, civil society, and members of Congress have raised an expansive set of privacy concerns, including its collection of Internet traffic for surveilling competitors; purchase of personal information from data brokers; tracking of non-Facebook users across the web; and harvesting of communications metadata from phones. These allegations raise new issues relevant to the consent decree that should be in the scope of the FTC's review.

The FTC ordered the consent decree in response to Facebook's repeated failures to address privacy risks, and put into place rules on how the company should act to protect users. If its investigation find that Facebook has violated the consent decree or engaged in further unfair or deceptive acts and practices, it should seek both monetary penalties that provide redress for consumers and impose stricter oversight on Facebook. The FTC should consider further measures that rigorously protects consumers, such as:

- data minimization standards that requires Facebook to retain and use data only for services expressly requested by users;
- limits on the combining and sharing of data between Facebook-owned services;

---

[6] "It's Time to Make Our Privacy Tools Easier to Find." Facebook. March 28, 2018. https://newsroom.fb.com/news/2018/03/privacy-shortcuts/

- transparency on the types of data that Facebook collects from users and from other sources, and to publicly account for how that data is used;
- restrictions on collection of data from its "social plug-ins," cross-device tracking, and or data brokers;
- appointment of a third-party monitor to oversee changes to Facebook's privacy and data use policies and practices, with periodic reinvestigation; and,
- organizational changes to ensure that privacy and data use is protected at all levels.

While the Cambridge Analytica revelations have raised awareness to Facebook's failure to provide users with adequate information or safeguards to protect privacy, many have raised legitimate and broad-reaching concerns about the company's practices beyond a single 'bad actor' problem. Mr. Zuckerberg has acknowledged that the incident was a breach of trust between Facebook and its users, a broken promise that requires redress for consumers and enforceable commitments that deter further breaches. It is time for the FTC to thoroughly and rigorously reassess Facebook's privacy practices and put into place rules that finally protect consumers.

Thank you for your attention to this important matter.

Sincerely,

Richard Blumenthal
United States Senate

Attachment 1

Global Science Research (GSR) Terms of Service

GSRApp APPLICATION END USER TERMS AND CONDITIONS

1. The Parties: This Agreement ("Agreement") is between Global Science Research ("We", "Us" or "GSR"), which is a research organisation registered in England and Wales (Number: 9060785) with its registered office based at Magdelene College, Cambridge, UK CB3 0AG, and the User of the Application ("You" or "User").

2. Agreement to Terms: By using GSRApp APP ("Application"), by clicking "OKAY" or by accepting any payment, compensation, remuneration or any other valid consideration, you consent to using the Application, you consent to sharing information about you with us and you also accept to be bound by the Terms contained herein.

3. Purpose of the Application: We use this Application as part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behaviour.

4. Data Security and Storage: Data security is very important to us. All data is stored on an encrypted server that is compliant with EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.

5. Your Statutory Rights: Depending on the server location, your data may be stored within the United States or in the United Kingdom. If your data is stored in the United States, American laws will regulate your rights. If your data is stored within the United Kingdom (UK), British and European Union laws will regulate how the data is processed, even if you live in the United States. Specifically, data protection and processing falls under a law called the Data Protection Act 1998. Under British and European Union law, you are considered to be a "Data Subject", which means you have certain legal rights. These rights include the ability to see what data is stored about you. Where data held in the EU is transferred to the United States, GSR will respect any safe harbour principles agreed between the United States Department of Commerce and the European Commission. The GSR Data Controller can be contacted by e-mail at alexbkogan@gmail.com.

6. Information Collected: We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network.

7. Intellectual Property Rights: If you click "OKAY" or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data. Specifically, agreement to these Terms also means you waive any copyright and other intellectual property rights in your data and contribution to GSR, and grant GSR an irrevocable, sublicenceable, assignable, non-

exclusive, transferrable and worldwide license to use your data and contribution for any purpose. You acknowledge that any and all intellectual property rights and database rights held in your data or contribution that is acquired by GSR or the Application will vest with GSR and that you will not have any claim in copyright, contract or otherwise. Nothing in this Agreement shall inhibit, limit or restrict GSR's ability to exploit, assert, transfer or enforce any database rights or intellectual property rights anywhere in the world. You also agree not attempt to appropriate, assert claim to, restrict or encumber the rights held in, interfere with, deconstruct, discover, decompile, disassemble, reconstruct or otherwise reverse-engineer the Application, the data collected by the Application or any other GSR technology, algorithms, databases, methods, formulae, compositions, designs, source code, underlying ideas, file formats, programming interfaces, inventions and conceptions of inventions whether patentable or un-patentable.

8. Informed Consent: By signing this form, you indicate that you have read, understand, been informed about and agree to these Terms. You also are consenting to have your responses, opinions, likes, social network and other related data recorded and for the data collected from you to be used by GSR. If you do not understand these Terms, or if you do not agree to them, then we strongly advise that you do not continue, do not click "OKAY", do not use the Application and do not to collect any compensation from us.

9. Variation of Terms: You permit GSR to vary these Terms from time to time to comply with relevant legislation, for the protection of your privacy or for commercial reasons. If you choose to provide us with your e-mail address, notice of any variation will be sent to that e-mail address. If you do not provide us with an e-mail address, you waive your right to be notified of any variation of terms.

10. Rights of Third Parties: A person who is not a Party to this Agreement will not have any rights under or in connection with it.

THISISYOURDIGITALLIFE APP APPLICATION END USER TERMS AND CONDITIONS

1. The Parties: This Agreement ("Agreement") is between Global Science Research ("We", "Us" or "GSR"), which is a research organisation registered in England and Wales (Number: 9060785) with its registered office based at St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS, and the User of the Application ("You" or "User").

2. Agreement to Terms: By using THISISYOURDIGITALLIF APP ("Application"), by clicking "OKAY" or by accepting any payment, compensation, remuneration or any other valid consideration, you consent to using the Application, you consent to sharing information about you with us and you also accept to be bound by the Terms contained herein.

3. Purpose of the Application: We use this Application to (a) provide people an opportunity to see their predicted personalities based on their Facebook information, and (b) as part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behaviour.

4. Data Security and Storage: Data security is very important to us. All data is stored on an encrypted server that is compliant with EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.

5. Your Statutory Rights: Depending on the server location, your data may be stored within the United States or in the United Kingdom. If your data is stored in the United States, American laws will regulate your rights. If your data is stored within the United Kingdom (UK), British and European Union laws will regulate how the data is processed, even if you live in the United States. Specifically, data protection and processing falls under a law called the Data Protection Act 1998. Under British and European Union law, you are considered to be a "Data Subject", which means you have certain legal rights. These rights include the ability to see what data is stored about you. Where data held in the EU is transferred to the United States, GSR will respect any safe harbour principles agreed between the United States Department of Commerce and the European Commission. The GSR Data Controller can be contacted by e-mail at info@globalscienceresearch.com.

6. Information Collected: We collect any information that you choose to share with us by using the Application. This may include, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network.

7. Intellectual Property Rights: If you click "OKAY" or otherwise use the Application or accept payment, you permit GSR to edit, copy, disseminate, publish, transfer, append or merge with other databases, sell, licence (by whatever means and on whatever terms) and archive your contribution and data. Specifically, agreement to these Terms also means you waive any copyright and other intellectual property rights in your data and contribution to GSR, and grant GSR an irrevocable, sublicenceable, assignable, non-exclusive, transferrable and worldwide license to use your data and contribution for any purpose. You acknowledge that any and all intellectual property rights and database rights held in your data or contribution that is acquired by GSR or the Application will vest with GSR and that you will not have any claim in copyright, contract or otherwise. Nothing in this Agreement shall inhibit, limit or restrict GSR's ability to exploit, assert, transfer or enforce any database rights or intellectual property rights anywhere in the world. You also agree not attempt to appropriate, assert claim to, restrict or encumber the rights held in, interfere with, deconstruct, discover, decompile, disassemble, reconstruct or otherwise reverse-engineer the Application, the data collected by the Application or any other GSR technology, algorithms, databases, methods, formulae, compositions, designs, source code, underlying ideas, file formats, programming interfaces, inventions and conceptions of inventions whether patentable or un-patentable.

8. Informed Consent: By signing this form, you indicate that you have read, understand, been informed about and agree to these Terms. You also are consenting to have your responses, opinions, likes, social network and other related data recorded and for the data collected from you to be used by GSR. If you do not understand these Terms, or if you do not agree to them, then we strongly advise that you do not continue, do not click "OKAY", do not use the Application and do not to collect any compensation from us.

9. Variation of Terms: You permit GSR to vary these Terms from time to time to comply with relevant legislation, for the protection of your privacy or for commercial reasons. If you choose to provide us with your e-mail address, notice of any variation will be sent to that e-mail address. If you do not provide us with an e-mail address, you waive your right to be notified of any variation of terms. 10. Rights of Third Parties: A person who is not a Party to this Agreement will not have any rights under or in connection with it.

- Privacy Policy

- Powered by **Global Science Research**

 St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS
Email: info@globalscienceresearch.com

Attachment 2

Sandy Parakilas Letter

Sandy Parakilas

Dear Senator Blumenthal,

In 2011 and 2012, I led the team responsible for overseeing Facebook's data policy enforcement efforts governing third-party application developers who were using Facebook's App Platform, and responding to violations of that policy.

In my first week on the job, I was told about a troubling feature of the App Platform: there was no way to track the use of data after it left Facebook's servers. That is, once Facebook transferred user data to the developer, Facebook lost all insight into or control over it. To prevent abuse, Facebook created a set of platform policies that forbade certain kinds of activity, such as selling the data or passing it to an ad network or data broker such as Cambridge Analytica.

Facebook had the following tools to deal with developers who abused the platform policies: it could call the developer and demand answers; it could demand an audit of the developer's application and associated data storage, a right granted in the platform policies; it could ban the developer from the platform; it could sue the developer for breach of the policies; or it could do some combination of the above. During my sixteen months at Facebook, I called many developers and demanded compliance, but I don't recall the company conducting a single audit of a developer where the company inspected the developer's data storage. Lawsuits and outright bans for data policy violations were also very rare.

Despite the fact that executives at Facebook were well aware that developers could, without detection, pass data to unauthorized fourth parties (such as what happened with Cambridge Analytica), little was done to protect users. A similar, well-publicized incident happened in 2010, where Facebook user IDs were passed by apps to a company called Rapleaf, which was a data broker. Despite my attempts to raise awareness about this issue, nothing was done to close the vulnerability. It was difficult to get any engineering resources assigned to build or maintain critical features to protect users.

Unfortunately, Facebook's failure to address this clear weakness, during my time there or after I left, led to Cambridge Analytica's misappropriation of tens of millions of Americans' data.

Sincerely,

Sandy Parakilas