

United States Senate  
WASHINGTON, DC 20510

October 10, 2018

The Honorable Joseph Simons  
Chairman  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Dear Chairman Simons:

We write to urge the FTC to immediately open an investigation into Google's exposure of private information from Google+ users and this alleged concealment in its handling of consumer data. The FTC should conduct a vigorous review whether the Google+ incident constitutes a breach of the company's consent decree or other commitments, and more broadly whether Google has engaged in deceptive acts and practices with respect to privacy. If the FTC finds problematic conduct, we encourage you to act decisively to end this pattern of behavior through substantial financial penalties and strong legal remedies

On October 8, 2018, Google announced that it had discovered a vulnerability associated with its social network product, Google+.<sup>1</sup> According to the company, a service used by developers, an Application Programming Interface (API), had exposed non-public profile information to others, such as name, email address, occupation, and age. This vulnerability could have potentially affected up to half a million Google users from 2015 and May 2018. While security problems are not uncommon, Google's concealment of this issue is troubling. According to the *Wall Street Journal*, Google hid the issue for six months to avoid public scrutiny about privacy practices.<sup>2</sup> The awareness and approval by Google management to not disclose represents a culture of concealment and opacity set from the top of the company.

Google has claimed that it "found no evidence that any developer was aware of this bug, or abusing the API, and we found no evidence that any Profile data was misused." These denials clash with the fact that Google has insufficient records to determine whether a breach occurred. According to its statement, the company only kept logs for two weeks. Google can only account for whether the vulnerability had been exploited in the weeks preceding its discovery. As such, we may never know the full extent of the damage caused by the failure to provide adequate controls and protection to users.

---

<sup>1</sup> Google. "Project Strobe: Protecting your data, improving our third-party APIs, and sunseting consumer Google+." Google Blog. October 08, 2018. <https://www.blog.google/technology/safety-security/project-strobe/>

<sup>2</sup> MacMillan, Douglas, and Robert McMillan. "Google Exposed User Data, Feared Repercussions of Disclosing to Public." *The Wall Street Journal*. October 08, 2018. <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194>.

The FTC has already put Google on notice, twice. In March 2011, Google agreed to a proposed settlement containing a consent decree after the FTC found that the company used deceptive tactics and violated its own privacy promises to consumers when it launched its first social network product, Google Buzz, in 2010.<sup>3</sup> Under the settlement, Google was barred from misrepresenting the privacy of personal information or the extent to which consumers may exercise control over the collection, use, or disclosure of covered information. The FTC also required Google 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.” Included in this program was the “regular testing or monitoring of the effectiveness of those privacy controls and procedures,” which would be audited by an independent third-party professional. Google is one of the rare companies that has violated a FTC consent decree, leading to a record fine for its circumvention of privacy protections in the web browser Safari.<sup>4</sup>

This failure to adequately disclose the Google+ vulnerability calls into question Google’s compliance with the consent decree’s requirements to respect privacy settings and protect private information. While the vulnerability was found in a recent initiative to audit platform security, Project Strobe, Google should have conducted such reviews long ago. The vulnerability was initially introduced in 2015, and Google has had at least six months to provide information to the public. This incident also demonstrates the need for stricter scrutiny of consent decree requirements. The accounting firm Ernst and Young conducted at least one mandated audit of Google’s privacy controls, but failed to uncover this vulnerability. Clearly, the FTC cannot continue to allow Google to select its own referee and to self-regulate.

Google now bears little resemblance to the company it was at the time of the consent decree, necessitating a renewed investigation into its privacy practices across its range of products and activities. Most consumers do not understand the level, granularity, and reach of Google’s data collection, a fact exacerbated by any possible breaches of trust. Researchers, civil society, and members of Congress have raised an expansive set of privacy concerns to the FTC, including its location monitoring; acquisition of sales data; tracking of non-Google users across the web; and scanning of emails. These allegations raise new issues relevant to the consent decree that should be in the scope of the FTC’s review.

We are strong supporters of the FTC and its consumer protection mission. We have long advocated for robust enforcement where consumer harm is present. Congress empowered the FTC with a broad consumer enforcement mandate because it wanted the FTC to evolve with the marketplace. It is time for the FTC to thoroughly reassess Google’s privacy practices and put into place rules that finally protect consumers. If its investigation finds that Google has violated the consent decree or engaged in further unfair or deceptive acts and practices, it should seek

---

<sup>3</sup> U.S. Federal Trade Commission. In the Matter of GOOGLE INC., a corporation. Docket No. C-4436. <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf>

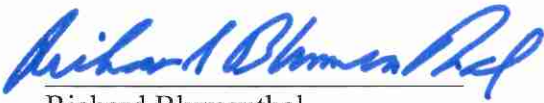
<sup>4</sup> Google Will Pay \$22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple’s Safari Internet Browser.” Federal Trade Commission. August 9, 2012. <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>.



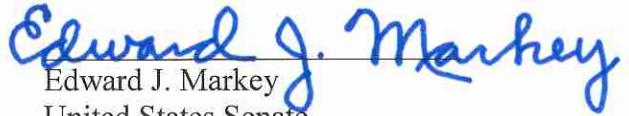
both monetary penalties that provide redress for consumers and impose stricter oversight on Google.

Thank you for your attention to this important matter.

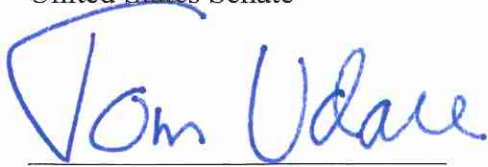
Sincerely,



Richard Blumenthal  
United States Senate



Edward J. Markey  
United States Senate



Tom Udall  
United States Senate