

ROGER WICKER, MISSISSIPPI
ROY BLUNT, MISSOURI
TED CRUZ, TEXAS
DEB FISCHER, NEBRASKA
JERRY MORAN, KANSAS
DAN SULLIVAN, ALASKA
DEAN HELLER, NEVADA
JAMES INHOFE, OKLAHOMA
MIKE LEE, UTAH
RON JOHNSON, WISCONSIN
SHELLEY MOORE CAPITO, WEST VIRGINIA
CORY GARDNER, COLORADO
TODD YOUNG, INDIANA

BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
AMY KLOBUCHAR, MINNESOTA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHÄTZ, HAWAII
EDWARD MARKEY, MASSACHUSETTS
CORY BOOKER, NEW JERSEY
TOM UDALL, NEW MEXICO
GARY PETERS, MICHIGAN
TAMMY BALDWIN, WISCONSIN
TAMMY DUCKWORTH, ILLINOIS
MAGGIE HASSAN, NEW HAMPSHIRE
CATHERINE CORTEZ MASTO, NEVADA

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: <http://commerce.senate.gov>

NICK ROSSI, STAFF DIRECTOR
KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

October 11, 2018

Mr. Sundar Pichai
Chief Executive Officer
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai:

Earlier this week, the *Wall Street Journal* reported¹ that, last March, Google discovered a vulnerability in its Google+ social network platform that had potentially left the private profile information of nearly 500,000 users exposed to app developers since 2015. Google reportedly opted not to disclose the existence of the issue at the time due, in part, to an inability to determine whether the vulnerability had in fact been exploited by any app developer to access private user data or which users were affected. But according to an internal memo cited in the article, a factor in Google's decision not to disclose the vulnerability was fear that doing so would draw "immediate regulatory interest," bring Google "into the spotlight alongside or even instead of Facebook despite having stayed under the radar throughout the Cambridge Analytica scandal," and "almost [guarantee] Sundar will testify before Congress."

Data privacy is an issue of great concern for many Americans who use online services. Particularly in the wake of the Cambridge Analytica controversy, consumers' trust in the companies that operate those services to keep their private data secure has been shaken. As the Senate Commerce Committee works toward legislation that establishes a nationwide privacy framework to protect consumer data, improving transparency will be an essential pillar of the effort to restore Americans' faith in the services they use.

It is for this reason that the reported contents of Google's internal memo are so troubling. At the same time that Facebook was learning the important lesson that tech firms must be forthright with the public about privacy issues, Google apparently elected to withhold information about a relevant vulnerability for fear of public scrutiny. We are especially disappointed given that Google's chief privacy officer testified before the Senate Commerce Committee on the issue of privacy on September 26, 2018—just two weeks ago—and did not take the opportunity to provide information regarding this very relevant issue to the Committee.

¹ Douglas MacMillan and Robert McMillan, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, WALL ST. J., Oct 8, 2018.

Google must be more forthcoming with the public and lawmakers if the company is to maintain or regain the trust of the users of its services. Therefore, we request your written responses to the following questions:

- 1) Please describe in detail when and how Google became aware of this vulnerability and what actions Google took to remedy it.
- 2) An October 8, 2018, Google blog post stated that the company found no evidence of misuse of profile data as a result of this Google+ vulnerability.² If Google discovers any such evidence in the future, will you commit to promptly informing this Committee, required law enforcement and regulatory agencies, and affected users?
- 3) Why did Google choose not to disclose the vulnerability, including to the Committee or to the public, until many months after it was discovered?
- 4) Did Google disclose the vulnerability to any federal agencies, including the Federal Trade Commission (FTC), prior to public disclosure?
- 5) Did Google disclose the vulnerability to its Independent Assessor tasked with examining Google's Privacy Program as part of the Agreement Containing Consent Order File No. 1023136 between Google and the FTC? If not, why not?
- 6) Are there similar incidents which have not been publicly disclosed?
- 7) Do you believe all users of free Google services who provide data to the company should be afforded the same level of notification and mitigation efforts as paid G Suite subscribers in the event of an incident involving their data?³
- 8) Please provide a copy of Google's internal memo cited in the *Wall Street Journal* article.

² Ben Smith, *Project Strobe: Protecting your data, improving our third-party APIs, and sunseting consumer Google+*, Google: The Keyword (Oct. 8, 2018), <https://blog.google/technology/safety-security/project-strobe/>.

³ "In its contracts with paid users of G Suite apps, Google tells customers it will notify them about any incidents involving their data 'promptly and without undue delay' and will 'promptly take reasonable steps to minimize harm.' That requirement may not apply to Google+ profile data, however, even if it belonged to a G Suite customer." Douglas MacMillan and Robert McMillan, *supra* note 1.


Mr. Sundar Pichai
October 11, 2018
Page 3

Please provide your written response as soon as possible, but by no later than 5:00 p.m. on October 30, 2018. Please also arrange for a staff briefing on this matter by contacting Jason Van Beek of the Committee staff at (202) 224-1251. Thank you for your prompt attention to this important matter.

Sincerely,



JOHN THUNE
Chairman
Committee on Commerce, Science,
and Transportation



ROGER F. WICKER
Chairman
Subcommittee on Communications,
Technology, Innovation, and the Internet



JERRY MORAN
Chairman
Subcommittee on Consumer Protection, Product
Safety, Insurance, and Data Security

cc: The Honorable Bill Nelson, Ranking Member