

November 13, 2013

Chairwoman Edith Ramirez
Commissioner Julie Brill
Commissioner Maureen Ohlhausen,
Commissioner Joshua Wright
The Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Re: NSA Data Collection from U.S. Companies

Dear Madam Chair and Members of the Federal Trade Commission,

We are writing to you regarding the news that the National Security Agency attacked the servers of Google and Yahoo and obtained the personal information of millions of consumers.¹ We believe that this development directly implicates the jurisdiction of the Federal Trade Commission and your specific orders regarding the steps that companies must take to safeguard consumer privacy.

We urge you to open an investigation to determine whether any failure by these companies to comply with the Commission's orders may have contributed to the improper disclosure of customer data.

We represent a wide range of consumer, privacy, and civil liberties organizations. We have previously written to you about the need to ensure that companies adopt best practices to safeguard the personal information that they collect. We have specifically recommended that companies adopt robust security practices, including the routine encryption of data, the minimization of data collection, and the deidentification of data where possible. And we have worked with your agency over many years to help ensure the development of policies and practices that help safeguard the sensitive, personal data obtained by US firms.

Several Internet companies are now subject to Federal Trade Commission orders requiring that they adopt "Comprehensive Privacy Programs" to safeguard the user information that they have obtained.² Better security standards have been the focus of several significant FTC settlements. Clearly these techniques were

¹ Barton Gellman and Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, WASH. POST, Oct. 30, 2013, available at http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

² See Google Inc. FTC Docket No. C-4336 (2011) (Decision and Order), <http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf>; Facebook, Inc., FTC Docket No. C-4365 (2012) (Decision and Order), <http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf>

inadequate if the NSA was able to obtain so much user data without the knowledge of the companies involved.

It is therefore vitally important for the Commission to open an investigation to determine whether there was adequate compliance with the Commission's prior orders.

Some have suggested that the Commission has no authority to investigate matters involving the conduct of the National Security Agency. That is plainly wrong. We are not writing to you regarding privacy matters that fall within the jurisdiction of some other federal agency, but specifically about conduct by US firms subject to orders of your agency that directly implicate the privacy interests of US consumers.

There are additional reasons that the Commission must immediately begin an investigation in the practices of these firms. These companies have represented that user data is only disclosed to law enforcement subject to a lawful process. But there is every reason now to believe that millions of consumer records were unlawfully obtained by the National Security Agency. Of course, once the records are in possession of these firms there is nothing that users can do to limit the subsequent improper release or avoid the misuse. And there is clearly no benefit to users in the improper and unlawful disclosure of their personal information

These are the necessary elements to establish the Commission's jurisdiction under Section 5 of the FTC Act.

Finally, the Commission should pursue this investigation because it routinely holds itself out as the defender of consumer privacy in the United States. It is inconceivable that when faced with the most significant breach of consumer data in U.S. history, the Commission could ignore the consequences for consumer privacy.

We urge you to immediately begin this investigation. The privacy of consumers should not be at risk because of the failure to comply with the Commission's earlier orders.

Respectfully,

/s/ Marc Rotenberg
Marc Rotenberg, Executive Director
Electronic Privacy Information Center
(EPIC)

/s/ Jeff Chester
Jeff Chester, Executive Director
Center for Digital Democracy (CDD)

/s/ John Simpson
John Simpson, Privacy Project Director
Consumer Watchdog

/s/ Beth Givens
Beth Givens, Director
Privacy Rights Clearinghouse

/s/ Susan Grant
Director of Consumer Protection
Consumer Federation of America

/s/ Robert Weissman
President
Public Citizen

/s/ Evan Hendricks
Editor and Publisher
Privacy Times

Cc:

Mark Pryor, Chairman, Senate Commerce Subcommittee on Consumer Protection,
Product Safety, and Insurance

Marco Rubio, Ranking Member, Senate Commerce Subcommittee on Consumer
Protection, Product Safety, and Insurance

Lee Terry, Chairman, House Energy Subcommittee on Commerce, Manufacturing
and Trade

Jan Schakowsky, Ranking Member, House Energy Subcommittee on Commerce,
Manufacturing and Trade