CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	CASE NO. 08-CV-4373-JSW **Declaration of Ashkan Soltani** The Honorable Jeffrey S. White

I, Ashkan Soltani, declare as follows:

1. I have been asked by plaintiffs' counsel to apply my expertise and experience to examine and analyze the evidence described below. In this declaration, I set forth my background, summarize my conclusions, and explain the basis and the reasoning supporting my conclusions. If called as a witness, I could and would testify to the matters stated herein.

2. Based on my expertise and experience, and after reviewing documents in this case, plaintiffs' use of cloud-based services such as webmail like Google's Gmail and Yahoo email increases the likelihood that their communications would be subject to collection as part of a surveillance network such as the one described by plaintiffs, even if that network were intended to intercept only communications with an international nexus.

BACKGROUND

3. I am a technology researcher and consultant with a focus on matters of privacy, cybersecurity, and policy. I have 20 years of experience in industry, government, and media, including work at the White House, Federal Trade Commission (FTC), Washington Post, and Wall Street Journal. Among other honors, my work as a co-author of the Washington Post's series on the National Security Agency (NSA) was awarded the 2014 Pulitzer Prize for Public Service.

4. I am currently the principal at Soltani, LLC, where since 2012 I have acted as a court-recognized technology expert and provide research, analysis, forensics, and testimony for clients such as the FTC and Attorneys General of California, New Jersey, Tennessee, and Ohio.

5. I received a Bachelor of Science degree in Cognitive Science with a minor in Computer Science from the University of California, San Diego in 1998. My studies focused on learning algorithms, collaboration, and data mining.

6. Between 1999 and 2005, I was a professional services consultant at Sophos, Inc. I consulted on network security and architecture for clients such as AT&T, Bank of America, Cisco, Amazon.com, NTT Japan, and the US Department of Homeland Security.

7. I received a Master of Information Management and Systems degree from the University of California, Berkeley in 2009.

8. My master's thesis, *KnowPrivacy*: *The Current State of Web Privacy, Data*

Collection, and Information Sharing, led me to serve as a consultant and investigative reporter for the Wall Street Journal's *What They Know* series, which examined the state of online tracking. I developed methods and tools to identify tracking technologies and their use, including demonstrating evidence of price discrimination online. The *What They Know* series was a finalist for the 2009 Pulitzer Prize for Investigative Reporting.

9. Between 2013 and 2014, I was the co-author of a series of articles documenting the extent of the NSA's surveillance programs for the Washington Post. The series was awarded the 2014 Pulitzer Prize for Public Service, the 2014 Loeb Award, and a 2013 Polk Award for National Security Reporting.

10. In 2010, I served as one of the first staff technologists at the FTC's Privacy and Identity Protection division. I conducted investigations into online security and privacy matters, including behavioral advertising, online tracking, and mobile privacy. I also assisted Commission staff in data gathering and forensics, analysis, reports, access letters, subpoenas, complaints and consent agreements on cases including Twitter, Google, Facebook, Myspace, and HTC.

11. Between 2014 and 2015, I served as the Chief Technologist at the FTC, where I was responsible for guiding the Commission on technology policy issues relating to privacy, security, and consumer protection. I created and staffed a new Office of Technology Research and Investigation to lead the agency's technical efforts.

12. Between 2015 and 2016, I was a Senior Advisor at the White House Office of Science and Technology Policy (OSTP). Serving under the White House Chief Technology Officer, I was responsible for developing United States policy on emerging technology issues including privacy, artificial intelligence, and big data.

13. The conclusions that I draw below rely on my professional training and experience, in addition to the following information, as explained in more detail below: documents and interviews I reviewed while reporting on the NSA for the Washington Post, and documents published by Google and Yahoo.

14. I am not receiving any compensation for my work as an expert in this matter.

SUMMARY OF CONCLUSION

15. My conclusion can be summarized as follows:

16. Plaintiffs' use of cloud-based applications, such as webmail like Google's Gmail and Yahoo email, increases the likelihood that their communications would be subject to collection as part of a surveillance network such as the one described by plaintiffs. For reasons related to availability, including disaster avoidance and server load, users' communications and associated data, including email accounts, are rarely stored in a single data center but often span across multiple, redundant geographic data centers. A single draft email message, even prior to it being sent, may be copied across multiple disparate computing systems in case an outage occurs at any single instance. As such, the distribution of emails between these data centers happens frequently and does not require that users send or receive email—and this distribution is designed specifically to traverse geographic borders in order to provide geographic redundancy. Therefore, even if defendants' Internet surveillance collection points are designed primarily to collect Internet traffic on foreign links or communications that originate or terminate outside the United States, it is likely that data belonging to users of cloud-based applications such as cloud email services passes through these collection points.

EXPLANATION OF THE BASIS FOR MY CONCLUSION

Large Providers of Cloud-Based Applications Store Data Such as the Contents of User Email Accounts Data Centers Located Around the World

17. As providers of cloud-based applications have grown larger, they have developed sophisticated systems to store and retrieve data including the contents of user email accounts.

18. A seminal paper published by Google in 2012 describes how one of these systems, a database named "Spanner," operates.[1] Spanner serves Google's goal of ensuring that data in the database has "high availability" and "low latency," that is, data is rarely if ever inaccessible, even in the face of failure of entire data centers, and that it can be retrieved and delivered to an end user with a minimum of delay. Spanner accomplishes these goals by breaking up data into segments or

[1] Google, *Spanner: Google's Globally-Distributed Database* (2012), https://static.googleusercontent.com/media/research.google.com/en//archive/spanner-osdi2012.pdf ("Spanner paper").

"shards," which it moves dynamically between Google data centers. It relies on distributed atomic clocks and GPS sensors to synchronize the movement of shards at a highly precise time scale, allowing changes to be made rapidly to the same set of data at different places in Google's network without leading to inconsistencies.

19. Data "shards" in the context of Google Spanner are not to be confused with IP "packets," which are the basic network data blocks in computer networking. Depending on the specific configuration, each "shard" may include significant portions of content, including email messages, chat conversations, and attachments. If the NSA or other outsiders intercepted a single shard, they could glean significant information about the communications, including an entire email or chat. Even if a shard did not contain a complete communication, interception of multiple shards would allow the entire communication to be reconstituted.

20. As a result, the location of individual shards in these data centers frequently changes. For example, "Spanner automatically reshards data across machines as the amount of data or the number of servers changes, and it automatically migrates data across machines (even across datacenters) to balance load and in response to failures."[2]

21. Spanner is used to manage the distribution of Google's Apps, including its Gmail email service. Therefore, shards of Google Apps user data, including the contents of Gmail users' accounts, are moved frequently between Google data centers as Spanner manages load on Google's network and ensures the availability of this data.

22. Google operates approximately 15 data centers located in North and South America, Europe and Asia.[3]

23. Yahoo operates similar databases to Spanner to manage and distribute data including the contents of email accounts among its global data centers.

24. Therefore, an email message belonging to a user of a cloud-based email service may move frequently between locations around the world even without action by the user.

---

[2] Spanner paper at 1.

[3] *See* Google, *Data center locations*, https://www.google.com/about/datacenters/inside/locations/index.html.

25. Due to the dynamic nature of Spanner and similar databases employed by Yahoo, it is likely that a program designed to conduct surveillance on the Internet backbone, even one aimed specifically at foreign Internet links or communications between individuals outside the United States would result in the collection of even purely domestic communications belonging to American users of cloud-based applications located in the United States.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

DATE: September 28, 2018

Ashkan Soltani