Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	File No.: EB-10-IH-4055
	)	
Google Inc.	)	NAL/Acct. No.: 201232080020
	)	
	)	FRNs: 0010119691, 0014720239
	)	

NOTICE OF APPARENT LIABILITY FOR FORFEITURE

Adopted: April 13, 2012 **Released: April 13, 2012**

By the Chief, Enforcement Bureau:

I. INTRODUCTION

1. Between May 2007 and May 2010, as part of its Street View project, Google Inc. (Google or Company) collected data from Wi-Fi networks throughout the United States and around the world.[1] The purpose of Google's Wi-Fi data collection initiative was to capture information about Wi-Fi networks that the Company could use to help establish users' locations and provide location-based services. But Google also collected "payload" data—the content of Internet communications—that was not needed for its location database project. This payload data included e-mail and text messages, passwords, Internet usage history, and other highly sensitive personal information.

2. When European data protection authorities investigated Google's Wi-Fi data collection efforts in 2010, the Company initially denied collecting payload data.[2] On May 14, 2010, however, Google publicly acknowledged that it had been "collecting samples of payload data from open (*i.e.*, non-password-protected) WiFi networks" but stated that it likely collected only fragmented data.[3] Google traced the collection of payload data to code that was "mistakenly" included in its Wi-Fi data collection software.[4] On October 22, 2010, Google acknowledged for the first time that "in some instances entire

---

[1] Google is a world leader in digital search capability. *See, e.g.*, Google Inc., Registration Statement (Form S-1), at 1 (Apr. 29, 2004), *available at* http://www.buec.udel.edu/pollacks/Acct351/handouts/SEC%20Form%20S-1%20filed%20by%20Google.pdf.

[2] *See* Posting of Peter Fleischer to Google European Public Policy Blog, http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html (Apr. 27, 2010, 1:01 p.m.) (Apr. 27 Google Blog Post) ("[W]e do not collect any information about householders, [and] we cannot identify an individual from the location data Google collects via its Street View cars.").

[3] Posting of Alan Eustace to The Official Google Blog, http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html (May 14, 2010, 4:44 p.m.) (May 14 Google Blog Post).

[4] Updated Posting of Alan Eustace to The Official Google Blog, http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html (June 9, 2010) (June 9 Google Blog Post); *accord* Posting of Brian McClendon to Google European Public Policy Blog, http://googlepolicyeurope.blogspot.com/2010/07/street-view-driving-update.html (July 9, 2010, 6:04 a.m.) (July 9 Google Blog Post); May 14 Google Blog Post ("Quite simply, it was a mistake.").

emails and URLs were captured, as well as passwords."[5] And finally, as described below, the Company provided evidence to the Federal Communications Commission (Commission) showing that the data collection [redacted].

3. Upon learning that Google had collected payload data, the Commission began examining whether Google's conduct violated provisions of the Communications Act of 1934, as amended (Communications Act or Act).[7] Based on that initial review, in November 2010 the Commission's Enforcement Bureau (Bureau) issued a Letter of Inquiry (LOI) that launched an official investigation into whether Google's data collection practices violated Section 705(a) of the Act.[8] The record developed in this investigation includes Google's written responses to questions from the Bureau, copies of relevant documents, and publicly available information. In addition, Bureau staff interviewed six individuals—five Google employees and an employee of Stroz Friedberg, a consulting firm Google retained to conduct forensic analysis of its Wi-Fi data collection software code. The Bureau also issued a subpoena to take the deposition of the Google engineer (Engineer Doe) who developed the software code that Google used to collect and store payload data.[9] Through counsel, however, Engineer Doe invoked his Fifth Amendment right against self-incrimination and declined to testify.

4. For many months, Google deliberately impeded and delayed the Bureau's investigation by failing to respond to requests for material information and to provide certifications and verifications of its responses. In this Notice of Apparent Liability for Forfeiture (NAL), we find that Google apparently willfully and repeatedly violated Commission orders to produce certain information and documents that the Commission required for its investigation. Based on our review of the facts and circumstances before us, we find that Google, which holds Commission licenses,[10] is apparently liable for a forfeiture penalty of $25,000 for its noncompliance with Bureau information and document requests.

5. At the same time, based on a careful review of the existing record and applicable law, the Bureau will not take enforcement action under Section 705(a) against the Company for its collection of payload data. There is not clear precedent for applying Section 705(a) of the Communications Act to the Wi-Fi communications at issue here. Moreover, because Engineer Doe permissibly asserted his constitutional right not to testify, significant factual questions bearing on the application of Section 705(a) to the Street View project cannot be answered on the record of this investigation.

---

[5] Posting of Alan Eustace to The Official Google Blog, http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html#!/2010/10/creating-stronger-privacy-controls.html (Oct. 22, 2010, 3:00 p.m.) (Oct. 22 Google Blog Post). "URL" is an acronym for Uniform Resource Locator, which means an Internet address.

[6] *See infra* paras. 22–23.

[7] 47 U.S.C. § 151 *et seq.*

[8] 47 U.S.C. § 605(a); Letter from P. Michele Ellison, Chief, FCC Enforcement Bureau, to Google Inc. (Nov. 3, 2010) (on file in EB-10-IH-4055).

[9] Throughout this Notice of Apparent Liability, we use aliases or redact the names of Google employees to protect their privacy.

[10] Google presently holds five active land mobile radio licenses (WQAK992, WQEN482, WQFX929, WQIR860, and WQIT645); one experimental license (WF2XYY); and three experimental Special Temporary Authorizations (WE9XTW, WF9XKU, and WF9XLG). In addition, Google Fiber, Inc. holds two satellite earth station licenses (E110145 and E110180), and one experimental Special Temporary Authorization (WF9XLK).

II. BACKGROUND

A. The Wiretap Act

6. Section 705(a) of the Act governs unauthorized publication or use of communications. The first sentence of Section 705(a) prohibits certain conduct "[e]xcept as authorized by chapter 119, title 18."[11] "Chapter 119, title 18" is a reference to the Wiretap Act,[12] which governs, among other things, the interception of electronic communications. The next two sentences of Section 705(a)—the provisions at issue in this investigation—state as follows:

> No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto.[13]

Congress amended Section 705(a) to cross-reference the Wiretap Act when it enacted the Wiretap Act as part of the Omnibus Crime Control and Safe Streets Act of 1968.[14] Although Congress incorporated the Wiretap Act proviso as an introductory clause to only the first sentence of Section 705(a), courts addressing the issue have determined that the proviso applies equally to all parts of Section 705(a).[15] In other words, case law supports that conduct authorized by the Wiretap Act is exempt from Section 705(a)'s prohibitions on the unauthorized interception and publication of radio communications and the unauthorized reception and use of interstate radio communications.

B. How Wi-Fi Networks Operate

7. Wi-Fi is a mechanism for wirelessly connecting electronic devices. Wi-Fi networks enable devices such as laptop computers, tablets, video game consoles, and smart phones to connect to the Internet and each other through a wireless network access point.[16] In a typical home configuration, the wireless access point is a wireless router connected to the Internet via coaxial cable, fiber, or DSL.[17] To facilitate communication with other electronic devices, wireless access points transmit a beacon that

---

[11] 47 U.S.C. § 605(a).

[12] 18 U.S.C. §§ 2510–2522.

[13] 47 U.S.C. § 605(a).

[14] *See* Pub. L. No. 90-351, 82 Stat. 197 (codified at 18 U.S.C. §§ 2510–2522 and scattered sections of 18 U.S.C.).

[15] *See Edwards v. State Farm Ins. Co.*, 833 F.2d 535, 540 (5th Cir. 1987); *United States v. Rose*, 669 F.2d 23, 26–27 (1st Cir. 1982); *United States v. Gass*, 936 F. Supp. 810, 812 (N.D. Okla. 1996).

[16] *See* Wi-Fi Alliance, Discover and Learn, http://www.wi-fi.org/discover_and_learn.php (last visited Apr. 9, 2012).

[17] *See* Wi-Fi Alliance, Simple Home Network, http://www.wi-fi.org/simple_home_network.php (last visited Apr. 9, 2012). Wi-Fi networks typically have a range of several hundred feet, but performance varies depending on obstructions and interference from other sources. *See* Wi-Fi Alliance, FAQs: What Is the Range of a Wi-Fi Network?, http://www.wi-fi.org/knowledge-center/faq/what-range-wi-fi-network (last visited Apr. 9, 2012).

provides basic information about a Wi-Fi network,[18] including (1) the medium access control (MAC) address, which is a unique numeric identifier for each wireless access point;[19] (2) the service set identifier (SSID), which is a name that identifies a particular wireless local area network (LAN);[20] and (3) transmission rates that the wireless access point supports. This information is unencrypted even if access to the Wi-Fi network is protected by a password.[21] Laptops, game consoles, and other devices with Wi-Fi capability use the information to establish a connection with a wireless access point to enable communication to and from the Internet.

C. Google's Wi-Fi Data Collection

8. Foreign privacy regulators began raising questions about Google's Street View program in early 2010. On April 27, 2010, Google noted on its European Public Policy Blog that there had been "a lot of talk about exactly what information Google Street View cars collect as they drive our streets."[22] The post, which in part purported to address concerns raised by data protection authorities in Germany, emphasized that "*Google does not collect or store payload data.*"[23]

9. On May 14, 2010, a new post on Google's official blog reported that "a statement made in a blog post on April 27 was incorrect."[24] The post explained that "it's now clear that we have been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks, even though we never used that data in any Google products."[25] The post then asserted, "[W]e will typically have collected only fragments of payload data because: our cars are on the move; someone would need to be using the network as a car passed by; and our in-car WiFi equipment automatically changes channels roughly five times a second."[26] In an attempt to explain why Google was collecting payload data, the post said, "Quite simply, it was a mistake."[27] The post claimed that the payload data

[18] *See, e.g.*, J. Geier, 802.11 Beacons Revealed, http://www.wi-fiplanet.com/tutorials/article.php/1492071 (last visited Apr. 10, 2012); [redacted]).

[19] *See* Wi-Fi Alliance, Glossary, http://www.wi-fi.org/knowledge-center/glossary (last visited Apr. 9, 2012).

[20] *See id.* A network operator can disable transmission of an SSID in the beacon, but the SSID nevertheless is included in requests by other Wi-Fi devices, such as laptops, to establish a connection with a wireless access point and in the responses thereto. *See* Google Document 11-4 at 4, 10, paras. 16, 52.b (June 3, 2010) (Stroz Friedberg Report), *available at* http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf.

[21] *See, e.g.*, Infrastructure Management Frame Protection (MFP) with WLC and LAP Configuration Example, http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008080dc8c.shtml (last visited Apr. 11, 2012).

[22] Apr. 27 Google Blog Post.

[23] *Id.* (emphasis added).

[24] May 14 Google Blog Post.

[25] *Id.*

[26] *Id.* Google has repeatedly claimed that the payload data it collected was fragmented because the software code changed channels at 0.2-second intervals, listening to each of the 11 Wi-Fi channels every 2.2 seconds. *See id.*; LOI Response at 11; Supplemental LOI Response at 10; *see also* Stroz Friedberg Report at 7, para. 28 (describing channel hopping).

[27] May 14 Google Blog Post.

collection code was the work of one engineer, that the Company never authorized payload data collection, and that the Street View project leaders did not want—and had no intention of using—payload data.[28] As soon as Google became aware of the payload data collection problem, the post assured, the Company grounded its Street View cars, segregated the data, and made the data inaccessible.[29] Google also "did not collect information travelling over secure, password-protected Wi-Fi networks."[30] Finally, the post noted that Google would ask "a third party to review the software at issue, how it worked and what data it gathered."[31]

10. Through counsel, Google retained Stroz Friedberg to evaluate the source code used in Google's global Wi-Fi data collection effort.[32] In an update posted on Google's official blog on June 9, 2010, Google stated that the Stroz Friedberg report had been completed and, "[i]n short, it confirms that Google did indeed collect and store payload data from unencrypted WiFi networks, but not from networks that were encrypted."[33] The update included a link to the report.[34]

11. Stroz Friedberg prepared its report based on a review of the code alone.[35] The report explains that, to facilitate the mapping of Wi-Fi networks, the source code, known as "gslite," used an

---

[28] *See id.*

[29] *See id.*

[30] *Id.*

[31] *Id.*

[32] *See* Stroz Friedberg Report at 1, para. 2.

[33] June 9 Google Blog Post. Google's April 27 blog post included a link to a submission Google made that day to "several national data protection authorities." Apr. 27 Blog Post; *see* Copy of Google's Submission Today to Several National Data Protection Authorities on Vehicle-Based Collection of WiFi Data for Use in Google Location Based Services, http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/googleblogs/pdfs/google_submission_dpas_wifi_collection.pdf (last visited Apr. 9, 2012). That submission included a vague statement about Google's ability to determine whether a Wi-Fi network is, or is not, unencrypted:

> It is possible to identify from the data received if an access point is encrypted—this may be included in the data sent in the frame header but in any event will be self-evident from the presence of encryption within the frames generally. However, while the information within the data frames will always reliably indicate to us if an access point is encrypted, we cannot reliably determine whether an access point *is not* encrypted. For example the data packet received by our equipment could be truncated or corrupted, meaning that we do not see the use of encryption within the broadcast. This does not, however, mean that the network is not encrypted—merely that we did not receive enough data to establish whether encryption was used or not.

Id. Although the meaning of that statement is unclear, Stroz Friedberg concluded that Google did *not* collect payload data from encrypted Wi-Fi networks. *See infra* para. 11. The premise that Google collected payload data only from unencrypted Wi-Fi networks is important to the Company's legal defense that its conduct was lawful under the Wiretap Act, and therefore lawful under Section 705(a) of the Communications Act. *See infra* para. 52.

[34] *See* June 9 Google Blog Post.

[35] *See* Stroz Friedberg Report at 1, para. 3; Interview with [redacted], in Washington, D.C. (Sept. 20, 2011) ([redacted] Interview). In an interview with Bureau staff, the Stroz Friedberg employee [redacted] verified that [redacted].

open-source "packet sniffing" program called Kismet[36] to capture, parse, and store MAC addresses, SSIDs, and other information about Wi-Fi networks.[37] According to the report, "All of this parsed header information is written to disk for frames transmitted over both encrypted and unencrypted wireless networks."[38] The report further explained, "The default behavior of gslite is to record all wireless frame data, with the exception of the bodies of encrypted 802.11 Data frames."[39] To determine whether a Wi-Fi network was encrypted, the gslite program searched for an "encryption flag."[40] "If the encryption flag identifie[d] the wireless frame as encrypted, the payload of the frame [was] cleared from memory and permanently discarded. If the frame's encryption flag identifie[d] the frame as not encrypted, the payload . . . [was] written to disk in a serialized format . . . ."[41] The report noted that if a user of an unencrypted network engaged in a password-protected Internet session, such as an online banking transaction, gslite would store any information captured from the session because the encryption flag would indicate that the network was unencrypted.[42] The information gathered would, however, be encrypted. In short, the software appears to have discarded data from encrypted networks, but not encrypted data transmitted over open networks. [redacted].

12. The Stroz Friedberg report states that on May 6, 2010, Google's Wi-Fi data collection program "was revised to disable *all* Data frame capture."[44] The report further states, "We have inspected the revised shell script and have confirmed that revision."[45] In an update posted on Google's official blog on July 9, 2010, a Company representative stated, "The Wi-Fi data collection equipment has been removed from our cars in each country and the independent security experts Stroz Friedberg have

[36] *See* Kismet, http://www.kismetwireless.net/ (last visited Apr. 9, 2012) (providing information about Kismet).

[37] *See* Stroz Friedberg Report at 2, para. 4. Because there are 11 Wi-Fi channels in the United States, "Kismet listens to each of the 11 channels for one fifth of a second, thus listening to every channel for one 0.2 second interval during each 2.2 second channel hopping cycle." *Id.* at 7, para. 28. In other countries there are as many as 14 Wi-Fi channels. *See id.* Wherever Street View cars used Kismet, the program hopped through all available channels in 0.2 second increments in a non-linear fashion. *See* [redacted] Interview.

[38] Stroz Friedberg Report at 4, para. 19. MAC addresses, SSIDs, and other information used to map the location of a Wi-Fi network are not encrypted even if the network itself is encrypted. *See supra* para. 7 and note 21.

[39] Stroz Friedberg Report at 5, para. 22. "Generally, the body of each Data frame contains the 'content' data of the encapsulated packet transmitted over the Internet, including such user-created data as email header information and bodies, URL requests, file transfers, instant messages, or any other communication over the Internet, as well as the addressing information for such transmissions." *Id.* at 3, para. 10.c.

[40] *Id.* at 4, para. 14.

[41] *Id.* at 5, 9, paras. 20, 42.

[42] *See id.* at 4, para. 14. The report specifically refers to hypertext transfer protocol secure (HTTPS) sessions, which are commonly used for online payment and banking transactions. *See* Wendy Boswell, *What Is HTTPS? What Does HTTPS Stand For?*, http://websearch.about.com/od/dailywebsearchtips/qt/dnt0513.htm (last visited Apr. 9, 2012).

[43] [redacted] Interview.

[44] Stroz Friedberg Report at 5, para. 22 n.2.

[45] *Id.*

approved a protocol to ensure any Wi-Fi related software is also removed from the cars before they start driving again."[46] Thus, when the Street View cars resumed driving, they no longer collected Wi-Fi data.

13. In October 2010, Google acknowledged that the payload data it had collected was more than simply fragments. At the end of a blog post on "[c]reating stronger privacy controls inside Google," a Company representative said:

> I would like to take this opportunity to update one point in my May blog post. When I wrote it, no one inside Google had analyzed in detail the data we had mistakenly collected, so we did not know for sure what the disks contained. Since then a number of external regulators have inspected the data as part of their investigations (seven of which have now been concluded). It's clear from those inspections that while most of the data is fragmentary, *in some instances entire emails and URLs were captured, as well as passwords.*[47]

In the same blog post, Google announced changes to its privacy and security practices to prevent similar incidents in the future.[48]

D. The Bureau's Investigation

14. On November 3, 2010, the Bureau sent Google a letter of inquiry (LOI) requesting information about the Company's Wi-Fi data collection activities to assess whether those activities violated Section 705(a).[49] The Bureau issued a supplemental LOI (Supplemental LOI) on March 30, 2011.[50] On August 18, 2011, the Bureau issued a demand letter (Demand Letter) ordering Google to provide complete responses to earlier requests and requesting additional information.[51] The Bureau issued a final supplemental LOI on October 21, 2011.[52] In addition to issuing written requests for information, the Bureau sought information by phone and in meetings and interviews with Google representatives.

---

[46] July 9 Google Blog Post.

[47] *See* Oct. 22 Google Blog Post (emphasis added).

[48] Google reported taking the following actions: (1) appointing a director of privacy to oversee engineering and product management; (2) enhancing its employee training program to include particular emphasis on "the responsible collection, use and handling of data"; and (3) requiring employees to participate in a new information security awareness program that provides guidance on security and privacy issues. *See id.* To ensure more careful review of design documents, Google reported that it had adopted a new process requiring every engineering project leader "to maintain a privacy design document for each initiative they are working on" that "will record how user data is handled and will be reviewed regularly by managers, as well as by an independent internal audit team." *Id.*; *accord* Google Document 11-6 & App. D; Supplemental LOI Response at 2–7.

[49] *See* LOI.

[50] *See* Letter from Theresa Cavanaugh, Acting Chief, Investigations and Hearings Division, FCC Enforcement Bureau, to Google Inc. (Mar. 30, 2011) (on file in EB-10-IH-4055).

[51] *See* Letter from P. Michele Ellison, Chief, FCC Enforcement Bureau, to Richard S. Whitt, Director and Managing Counsel for Telecom and Media Policy, Google Inc., and E. Ashton Johnston, Counsel to Google Inc. (Aug. 18, 2011) (on file in EB-10-IH-4055).

[52] Letter from Theresa Cavanaugh, Acting Chief, Investigations and Hearings Division, FCC Enforcement Bureau, to Google Inc. (Oct. 21, 2011) (on file in EB-10-IH-4055).

15. We note that several countries, including Canada,[53] France,[54] and the Netherlands,[55] have determined that Google's collection of payload data violated their data protection, online privacy, or similar laws and regulations. In the United States, the Federal Trade Commission (FTC) initiated an inquiry in the summer of 2010. On October 27, 2010, the FTC closed its inquiry without taking action against Google.[56] State attorneys general have conducted a joint investigation that is ongoing.[57]

1. Google's response to the LOI

16. The Bureau's initial LOI required Google to provide specified information about its Wi-Fi data collection activities that would enable Commission staff to assess whether those activities violated Section 705(a) of the Act.[58] The focus of the first LOI was on how Google collected Wi-Fi data, what data they got, and whether the company had examined or used that data in any way. The LOI directed Google to provide certain information in narrative form, as well as copies of all documents (including e-mail) that supported the Company's narrative responses.[59] The LOI also required Google to identify the individuals responsible for authorizing the collection of Wi-Fi data, and to identify any employees who had reviewed or analyzed Wi-Fi communications collected by the Company.[60] In addition, the LOI directed Google to accompany its response with

> an affidavit or declaration under penalty of perjury, signed and dated by an authorized officer of the Company with personal knowledge of the representations provided in Google's response, verifying the truth and accuracy of the information therein and that all of the information and/or documents

---

[53] *See generally* Office of the Privacy Comm'r of Canada, PIPEDA Report of Findings No. 2011-001, Google Inc. WiFi Data Collection (2011) (OPC Report), *available at* http://www.priv.gc.ca/cf-dc/2011/2011_001_0520_e.cfm.

[54] *See generally* Commission Nationale de l'Informatique et des Libertés Decision No. 2011-035 of the Restricted Committee Imposing a Financial Penalty on the Company Google Inc. (2011) (CNIL Decision), *available at* http://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000023733987. Citations in this NAL to the CNIL Decision are to the original French language document, as translated by Commission staff.

[55] *See generally* Dutch Data Protection Authority, Final Findings, Investigation into the collection of Wifi data by Google using Street View cars (Dec. 7, 2010) (DDPA Decision), *available at* http://www.dutchdpa.nl/downloads_overig/en_pb_20110811_google_final_findings.pdf.

[56] *See* Letter from David Vladeck, Director, FTC Bureau of Consumer Protection, to Albert Gidari, Counsel to Google Inc. at 2 (Oct. 27, 2010), available at http://www.ftc.gov/os/closings/101027googleletter.pdf.

[57] *See, e.g.*, Tom Krazit, *Connecticut Heads Up 30-State Google Wi-Fi Probe*, C-NET, June 21, 2010, http://news.cnet.com/8301-30684_3-20008332-265.html. In addition, private citizens have filed numerous class action lawsuits against Google alleging that the Company violated federal wiretapping laws when it captured personal information from Wi-Fi networks. Eight of those class actions have been consolidated in the U.S. District Court for the Northern District of California. *See In re Google Inc. Street View Elec. Commc'ns Litig.*, 733 F. Supp. 2d 1381, 1382 (J.P.M.L. 2010). On June 29, 2011, that court granted in part and denied in part Google's motion to dismiss for failure to state a claim upon which relief may be granted. *See In re Google Inc. Street View Elec. Commc'ns Litig.*, 794 F. Supp. 2d 1067, 1086 (N.D. Cal. 2011).

[58] 47 U.S.C. § 605(a); *see* LOI.

[59] *See* LOI at 4.

[60] *See id.* at 3.

> requested . . . which [were] in Google's possession, custody, control, or knowledge [had] been produced.[61]

17. When Google responded to the LOI on December 10, 2010, it produced only five documents.[62] Google's document production included no e-mails, and the Company admitted that it had "not undertaken a comprehensive review of email or other communications"[63] because doing so "would be a time-consuming and burdensome task."[64] Google also failed to identify any of the individuals responsible for authorizing its collection of Wi-Fi data or any employees who had reviewed or analyzed Wi-Fi communications collected by the Company.[65] Indeed, Google redacted the names of its engineers from the few documents that were produced.[66] The Company asserted that identifying its employees "at this stage serves no useful purpose with respect to whether the facts and circumstances give rise to a violation" of the Act.[67]

18. Google further failed to supply the required verification of its LOI response. Although Google submitted a declaration signed [redacted],[68] that declaration did not satisfy the LOI because the person who signed it had no direct involvement in the Street View Wi-Fi data collection project and did not assert personal knowledge of the information that Google provided in response to the LOI.[69] In a telephone call on January 6, 2011, the Bureau advised Google that its declaration was deficient and directed the Company to submit a compliant version; Google did not do so.[70]

19. The information that Google eventually provided revealed the following facts regarding the Company's Wi-Fi data collection program, which we recite in detail because of the widespread interest in this matter and, particularly, the implications of Google's collection of payload data for Wi-Fi users who are concerned about the security of their Wi-Fi enabled communications.

20. In 2006, Google was preparing to deploy cars to collect images for Google Street View, which gives users of Google Maps and Google Earth the ability to view street-level images of structures

---

[61] *Id.* at 4–5.

[62] *See* Responses of Google Inc. to Letter of Inquiry, File No. EB-10-IH-4055 (Dec. 10, 2010) (LOI Response) (enclosing Google Documents 11-1 through 11-5). Google redacted information in documents 11-1 through 11-3. Google redacted Document 11-3—the software code—in an inappropriate manner that made it impossible to know where the redactions occurred.

[63] LOI Response at 1.

[64] *Id.* at 12. Google also requested "forbearance in the preparation of a privilege log." *Id.* at 1.

[65] *See id.* at 6–7.

[66] *See id.* at 12.

[67] *Id.* In a supplemental LOI response on December 20, 2010, Google [redacted]. *See* Second Supplement to Responses of Google Inc. to Letter of Inquiry, File No. EB-10-IH-4055 at 1 (Dec. 20, 2010).

[68] *See* LOI Response, Declaration of [redacted] (Dec. 9, 2010).

[69] *See id.*

[70] *See* Demand Letter at 2.

and land adjacent to roads and byways around the globe.[71] Each car was furnished with special equipment to capture and store 360-degree digital images, which are correlated with specific coordinates on maps. Street View enables users to "explore world landmarks, view natural wonders, navigate a trip, go inside restaurants and small businesses - and now even visit the Amazon!"[72]

21. [redacted] "wardriving," which is the practice of driving streets and using equipment to locate wireless LANs using Wi-Fi, such as wireless hotspots at coffee shops and home wireless networks.[73] By collecting information about Wi-Fi networks (such as the MAC address, SSID, and strength of signal received from the wireless access point) and associating it with global positioning system (GPS) information, companies can develop maps of wireless access points for use in location-based services.[74] To design the Company's program, Google tapped Engineer Doe, [redacted].[75] As described further below, Engineer Doe developed Wi-Fi data collection software code that, in addition to collecting Wi-Fi network data for Google's location-based services, would collect payload data [redacted]. In response to the LOI, Google made clear for the first time [redacted].

22. One of the five documents Google produced in response to the LOI was a design document [redacted]. The design document showed that, in

[71] To date, Google has collected Street View images in North America, Brazil, Europe, the Middle East, southern Africa, Asia, Australia, and New Zealand. *See* Google Inc., Where Is Street View Available?, http://maps.google.com/help/maps/streetview/learn/where-is-street-view.html (last visited Apr. 9, 2012).

[72] *See* Google Maps, Street View, http://maps.google.com/intl/en/help/maps/streetview/#utm_campaign=en&utm_medium=van&utm_source=en-van-na-us-gns-svn (last visited Apr. 10, 2012).

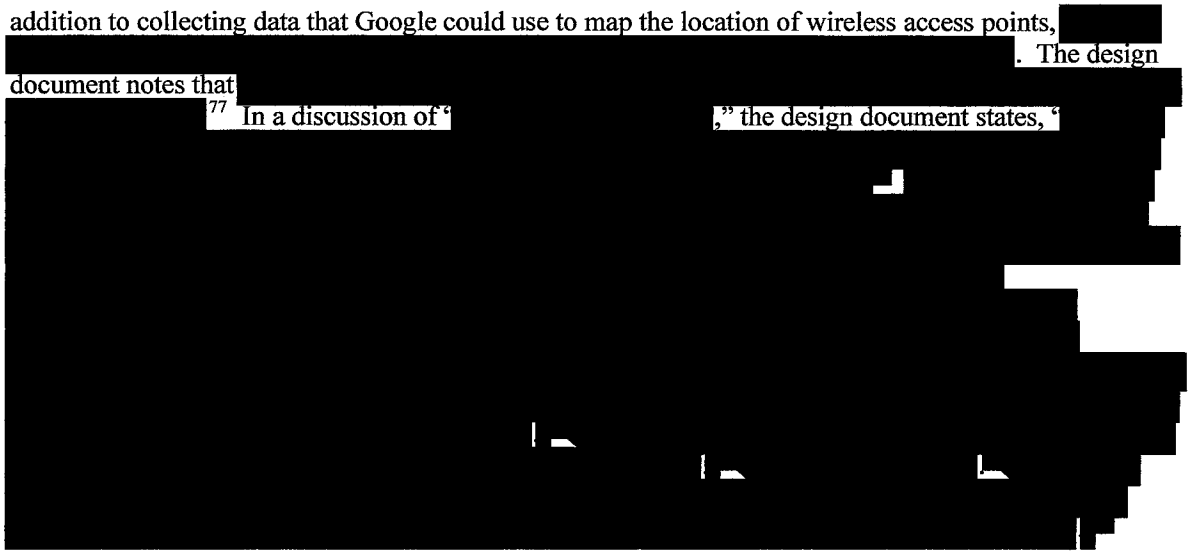
[73] *See* Google Document 11-7 ("[redacted]"). For a description of wardriving, see Wireless LAN Security, 802.11/Wi-Fi Wardriving & Warchalking, http://www.wardrive.net (last visited Apr. 9, 2012).

[74] *See* LOI Response at 3–4. For example, when a smart phone user seeks information about nearby restaurants or movie theaters, a service provider can supply the requested information by determining the user's approximate location based on proximity to known wireless access points and other available location information, such as GPS coordinates. *See id.*

[75] Engineer Doe worked on the Street View project [redacted]. *See id.*; Declaration of [redacted] at paras. 2–3 (Aug. 30, 2011) ([redacted] Decl.); Supplemental LOI Response at 11; [redacted].

[76] Google initially failed to produce all versions of the design document. In its response to the LOI, Google produced a copy that says, "[redacted]." *See* Google Document 11-1 at 1. In its response to the Bureau's Supplemental LOI, Google stated that [redacted]. *See* Responses of Google Inc. to Supplemental Letter of Inquiry, File No. EB-10-IH-4055 at 8 (Apr. 14, 2011) (Supplemental LOI Response). That statement suggested [redacted]. In its Demand Letter, the Bureau directed Google to produce copies of all prior and subsequent versions of the [redacted] design document, including the version completed on [redacted]. Demand Letter at 3. On September 7, 2011, Google produced five prior versions. *See* Google Documents 11-16 to 11-20.

addition to collecting data that Google could use to map the location of wireless access points, [redacted]. The design document notes that [redacted][77] In a discussion of "[redacted]," the design document states, "[redacted]



23. In addition to the design document, Google also produced to the Bureau a copy of the software that Engineer Doe developed, which independently revealed [redacted]. [redacted] "[d]iscard just the body of encrypted frames." [redacted] intended to store everything *but* the body of encrypted frames, including the content of communications over unencrypted Wi-Fi networks.

24. Using the code that Engineer Doe developed, Google collected payload data from unencrypted Wi-Fi networks in the United States between January 2008 and April 2010.[84] During that period, Street View cars driving in the United States collected a total of approximately [redacted] of payload data—[redacted].[85] Later in the investigation, we learned that after initially

[77] Google Document 11-20 at 2. [redacted]. *See* Google Document 11-1 at 1.

[78] Google Document 11-20 at 10 (emphasis added); *accord* Google Document 11-1 at 6.

[79] Google Document 11-20 at 10; *accord* Google Document 11-1 at 6.

[80] Google Document 11-20 at 10; *accord* Google Document 11-1 at 6.

[81] *See* Supplemental LOI Response at 2.

[82] Google Document 11-20 at 1; *accord* Google Document 11-1 at 1.

[83] Google Document 11-3; Stroz Friedberg Report at 12, para. 57.

[84] *See* LOI Response at 3. In its Supplemental LOI Response, the Company explained that "[redacted] Wi-Fi collection hardware and software was first launched in May 2007 and continued until early May 2010 when Google discovered the payload collection and ceased any Wi-Fi collection via Street View cars." Supplemental LOI Response at 8.

[85] *See* LOI Response at 9.

storing all Wi-Fi data in machine-readable format on a hard disk on each Street View car,[86] [redacted].[87]

25. The Bureau's LOI directed Google to provide a copy of or access to the Wi-Fi communications that Google collected.[88] Google argued that [redacted].[89] The Bureau did not further pursue access to the data because authorities in other countries—including Canada, France, and the Netherlands—inspected payload data that Google collected within their borders and described the nature of that data in public reports. Those investigations confirmed that Google collected large amounts of payload data, including data that was both intact and personally identifiable, as described below.

- *Canada*. In 2010, technical experts from the Office of the Privacy Commissioner of Canada (OPC) examined a sample of payload data that Google collected in Canada. The sample "revealed, among other information, the full names, telephone numbers, and addresses of many Canadians. We also found complete email messages, along with email headers, IP addresses, machine hostnames, and the contents of cookies, instant messages and chat sessions."[90] The OPC was "troubled to have found instances of particularly sensitive information, including computer login credentials (i.e., usernames and passwords), the details of legal infractions, and certain medical listings."[91]

- *France*. On March 18, 2011, the Commission Nationale de l'Informatique et des Libertés (CNIL) issued a decision based on its investigation of Google's Wi-Fi data collection. From a sample of payload data Google collected in France, the CNIL was able to isolate 656 megabytes of data related to Internet navigation, including passwords for Internet sites and data relating to online dating and pornographic sites.[92] Analysis of the data permitted the CNIL "to determine with a great deal of precision the type of sites consulted, the passwords permitting access to them and the geographic location of the user."[93] The CNIL isolated 6 megabytes of data related to electronic mail, including 72

[86] LOI Response at 7. Google has represented that the data is unreadable without proprietary Google software. *See id.*

[87] *See* Telephone Interview with [redacted], Google Inc., in Mountain View, Cal. (Oct. 6, 2011) ([redacted] Interview); Interview with [redacted], Google Inc., in Mountain View, Cal. (Sept. 28, 2011) ([redacted] Interview).

[88] *See* LOI at 4.

[89] Google claimed that '[redacted]" LOI Response at 9. [redacted]. *See id.* at 10.

[90] OPC Report at 7, para. 17.

[91] *Id.* at 7, para. 18. The OPC concluded that although Google collected the payload data from unencrypted Wi-Fi networks and some of the data was fragmented, "it [was] impossible to conceive that a reasonable person would have considered such collection appropriate in the circumstances." *Id.* at 8, para. 21.

[92] CNIL Decision at 10.

[93] *Id.* ("Quant à l'analyse des données de contenu, elle a permis de déterminer avec une grande précision la nature des sites consultés, les mots de pass permettant d'y accéder et l'emplacement géographique de l'utilisateur.").

e-mail passwords and 774 distinct e-mail addresses.[94] For example, the CNIL found "an exchange of e-mails between a married woman and man, both seeking an extra-marital relationship," from which first names, e-mail addresses, and physical addresses could be discerned.[95] The CNIL also found web addresses that revealed the sexual preferences of consumers at specific residences.[96]

- *The Netherlands*. The Dutch Data Protection Authority (DDPA) reviewed payload data collected by Google in the Netherlands over a two-year period[97] and concluded that "[t]he recorded data are not meaningless fragments. It is factually possible to capture 1 to over 2,500 packets per individual user in 0.2 seconds. Moreover, the car may have captured a signal from a single Wifi router several times . . . ."[98] In addition, the DDPA found that Google had captured a broad assortment of Internet traffic, including e-mails, chat traffic, URLs, passwords, and video and audio files, some of which was highly sensitive.[99] The DDPA also concluded that it was "possible to link several *packets* from 1 Internet user to each other, and in doing so construct an accurate picture of the communication of an often identifiable user."[100]

In interviews and correspondence with the Bureau, Google representatives acknowledged that [redacted][101] [redacted], we believe the payload data Google collected in the United States is similar to what foreign authorities have described.

26. In response to the first LOI, Google stated that its employees reviewed payload data on only two occasions. First, [redacted] Engineer Doe examined payload data to determine whether it might be useful [redacted]. Second, when senior corporate officials became aware in 2010 that the Company had collected payload data from unencrypted Wi-Fi networks around the world, Google's "engineering staff confirmed that this was the case" by inspecting the data.[102] Google represents that "[i]n no other instance has any employee, agent, officer, or director of Google analyzed the collected data."[103]

---

[94] *See id.*

[95] *Id.* at 11 ("Un échange de courriels entre une femme et un homme mariés, cherchant tous deux une relation extraconjugale.").

[96] *See id.*

[97] *See* DDPA Decision at 8.

[98] *Id.*

[99] *See* DDPA Decision at 12–15.

[100] *Id.* at 8; *see id.* at 12, 40.

[101] *See, e.g.*, [redacted] Interview; [redacted] Interview; [redacted] Interview; Sept. 2011 Response at 5.

[102] LOI Response at 7.

[103] *Id.*

2. Google's response to the Supplemental LOI

27. On March 30, 2011, the Bureau sent Google the Supplemental LOI, which focused primarily on Google's internal privacy controls and how Engineer Doe's software was deployed. The LOI also addressed the Company's failure to respond fully to the first LOI. In view of Google's failure to produce any e-mails in response to the initial LOI and the Company's admission that it had not attempted a comprehensive review of its employees' e-mails, the Supplemental LOI directed the Company "to provide a full response to the [original] LOI that reflects a comprehensive search of all materials within the Company's possession, as instructed in the original LOI," as well as to "provide complete responses, certifying that a complete search was conducted."[104] In addition, the Supplemental LOI reiterated the demand that Google identify the individuals responsible for authorizing the Company's collection of Wi-Fi data.[105] The Supplemental LOI also directed the Company, for a third time, to provide a compliant declaration attesting to the completeness and veracity of its LOI response.[106]

28. Google submitted its response to the Supplemental LOI on April 14, 2011. Google produced eight e-mails responsive to the Bureau's inquiries, identified some individuals who had worked on the Street View project, and produced documents that revealed the names of others.[107] Google failed, however, to provide the required certification that it had conducted "a comprehensive search of all materials within the Company's possession."[108] Similarly, Google failed to furnish a compliant declaration with respect to the veracity and completeness of its LOI response as a whole.[109]

29. At a meeting with Google on May 18, 2011, the Bureau reiterated once more its concern regarding the Company's failure to provide a compliant declaration. The Bureau explained that without one, the Commission could not place confidence in the completeness and veracity of Google's submissions.[110] Again, the Company failed to provide a compliant declaration.

30. In response to the Supplemental LOI, Google expanded upon [redacted]. Google explained that [redacted]." Google further stated that [redacted]

[104] Supplemental LOI at 4. The Bureau also directed Google "to provide the privilege log as instructed in the LOI." *Id.*

[105] *See id.* at 3.

[106] *See id.* at 4–5.

[107] *See* Google Documents 11-7 to 11-10, 11-12 to 11-15; Supplemental LOI Response at 10–11. The Company also produced unredacted copies of Google Documents 11-1 through 11-3.

[108] Supplemental LOI at 4.

[109] *See generally* Supplemental LOI Response.

[110] *See* Demand Letter at 2.

[111] Supplemental LOI Response at 9. Google subsequently produced a copy of [redacted]. *See* Letter from E. Ashton Johnson, Counsel to Google Inc., to Theresa Cavanaugh, Acting Chief, Investigations and Hearings Division, FCC Enforcement Bureau at Attachment 2 (June 3, 2011) (on file in EB-10-IH-4055).

[redacted].”[112] According to Google, Engineer Doe “did not access [the payload data] again.” Copies of e-mails that Google produced in response to the Supplemental LOI showed that [redacted] Google’s response to the Supplemental LOI further revealed that [redacted].

31. [redacted] we [redacted].”

3. Google’s response to the Demand Letter

32. Because there continued to be deficiencies in Google’s responses to the Bureau’s inquiries, on August 18, 2011, the Bureau sent Google the Demand Letter requiring complete responses under threat of subpoena. Regarding Google’s continued failure to provide a compliant declaration attesting to the veracity and completeness of its responses to the Commission’s inquiries, the Demand Letter stated, “The Bureau . . . again directs the Company, for a fifth time, to provide an affidavit or declaration, signed and dated by an authorized officer of the Company with personal knowledge, attesting to the accuracy and completeness of the Company’s LOI responses.”[120] The Demand Letter made clear

[112] Supplemental LOI Response at 9; *accord* LOI Response at 7.

[113] LOI Response at 7. The Bureau could not verify Google’s representations regarding Engineer Doe because, as noted above, he declined to testify.

[114] *See* Google Document 11-9.

[115] *See id.*; Supplemental LOI Response at 8.

[116] Google Document 11-13. Data frames contain the content of Internet communications, such as Internet addresses, the body of e-mails, and instant messages. *See* Stroz Friedberg Report at 3, para. 10.c.

[117] Google Document 11-14. “MapReduce” is a programming model developed within Google as a mechanism for processing large amounts of raw data. *See* Google Code University, Introduction to Parallel Programming and MapReduce, http://code.google.com/edu/parallel/mapreduce-tutorial.html (last visited Apr. 9, 2012).

[118] Google Document 11-14 (emphasis added).

[119] *Id.*

[120] Demand Letter at 2–3. The Demand Letter further directed that “[i]f such officer is relying on the personal knowledge of any other individual, . . . provide separate affidavits or declarations of each such individual with (continued....)

that if the Company continued to refuse to comply, the Bureau would have no choice but to compel compliance.[121]

33. On September 7, 2011, Google provided declarations from nine employees who worked on the Street View project.[122] Those declarations served, for the first time, [redacted] By supplying support from individuals with personal knowledge, the employee declarations—and a revised officer declaration that Google submitted at the same time—also served at last to verify the completeness and accuracy of Google's submissions in the manner the Bureau had directed.

4. Interviews of Google and Stroz Friedberg employees

34. The Bureau subsequently interviewed five of the employees who submitted declarations, along with a representative of Stroz Friedberg, the consulting firm Google retained to analyze its Wi-Fi data collection software code.[123] Those interviews focused in large part on [redacted].

35. In interviews and declarations, managers of the Street View project and other Google employees who worked on the project told the Bureau they [redacted].[124] A senior manager of Street View said [redacted].[125] One engineer remembered [redacted].[126]

36. During interviews with Bureau staff, Google employees stated that [redacted]

(Continued from previous page) ———————————
personal knowledge that identify clearly the responses to which each affiant or declarant with such personal knowledge is attesting." *Id.*

[121] *Id.* at 5.

[122] *See* Letter from Richard S. Whitt, Director and Managing Counsel for Telecom and Media Policy, Google Inc., to P. Michele Ellison, Chief, FCC Enforcement Bureau at 2–3 (Sept. 7, 2011) (on file in EB-10-IH-4055) (Sept. 2011 Response) (describing the enclosed declarations).

[123] Google refused the Bureau's request to record those interviews.

[124] *See* [redacted] Interview; [redacted] Interview; [redacted] Interview; Interview with [redacted], Google Inc., in Washington, D.C. (Sept. 20, 2011) ([redacted] Interview); Declaration of [redacted] at para. 3 (Aug. 31, 2011) ([redacted] Decl.); Declaration of [redacted] at paras. 3–4 (Aug. 31, 2011) ([redacted] Decl.); Declaration of [redacted] at para. 2 (Aug. 30, 2011) ([redacted] Decl.); [redacted] Decl. at para. 4; Declaration of [redacted] at para. 3 (Aug. 30, 2011) ([redacted] Decl.).

[125] *See* [redacted] Interview.

[126] *See* [redacted] Decl. at para. 4.

[redacted].[127] [redacted].

37. [redacted]. In both his written declaration and his interview with Bureau staff, the engineer characterized [redacted].

38. [redacted]." A manager of the Street View project estimated [redacted].[135] [redacted].

39. [redacted] et

---

[127] *See* [redacted] Interview; [redacted] Interview. [redacted]" *See* [redacted] Interview.

[128] *See* Telephone Interview with [redacted] Google Inc., in Mountain View, Cal. (Oct. 6, 2011) ([redacted] Interview).

[129] *See* [redacted] Interview; Google Document 18-46.

[130] *See* [redacted] Interview.

[131] *See id.*; [redacted] Decl. at para. 2.

[132] *See* [redacted] Interview.

[133] *See id.*; [redacted] Decl. at para. 2.

[134] *See* [redacted] Interview; Declaration of [redacted] at para. 2 (Aug. 31, 2011) ([redacted] Decl.).

[135] *See* [redacted] Interview.

[136] *See* [redacted] Decl. at para. 3.

[137] *See* [redacted] Decl. at para. 2.; [redacted] Decl. at paras. 3–4.

[redacted].

III. DISCUSSION

40. Under Section 503(b)(1)(B) of the Communications Act, any person whom the Commission determines to have willfully or repeatedly failed to comply with a provision of the Act or any Commission rule, regulation, or order "shall be liable to the United States for a forfeiture penalty."[139] Section 312(f)(1) of the Act defines willful as "the conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate" the law.[140] The legislative history to Section 312(f)(1) clarifies that this definition of willful applies to both Sections 312 and 503(b) of the Act,[141] and the Commission has so interpreted the term in the Section 503(b) context.[142] The Commission may also assess a forfeiture penalty for violations that are merely repeated, and not willful.[143] "Repeated" means that the act was committed or omitted more than once, or lasts more than one day.[144] To impose such a forfeiture penalty, the Commission ordinarily must issue a notice of apparent liability for forfeiture, and the person against whom the notice has been issued must have an opportunity to show, in writing, why no such forfeiture penalty should be imposed.[145] The Commission will then issue a forfeiture order if it finds, based on the evidence, that the person has violated the Act, a rule, or a Commission order.[146]

41. In this NAL, we find that Google is apparently liable for a forfeiture penalty of $25,000 based on the Company's apparent failure to timely (1) provide compliant declarations verifying the completeness and accuracy of its LOI responses for a period of almost nine months, (2) identify Google employees with knowledge of relevant facts, and (3) search for and produce any e-mails.

---

[138] *See* [redacted] Interview; [redacted] Interview; [redacted] Interview; [redacted] Interview; [redacted] Interview; [redacted] Decl. at para. 3; [redacted] Decl. at para. 2; Declaration of [redacted] at para. 3 (Aug. 31, 2011); [redacted] Decl. at paras. 3–4; Declaration of [redacted] at para. 3 (Aug. 30, 2011); Declaration of [redacted] at para. 3 (Aug. 30, 2011); [redacted] Decl. at paras. 4–5; [redacted] Decl. at para. 3.

[139] 47 U.S.C. § 503(b)(1)(B).

[140] 47 U.S.C. § 312(f)(1).

[141] *See* H.R. Rep. No. 97-765, 97th Cong. 2d Sess. 51 (1982).

[142] *See, e.g., So. Cal. Broadcasting Co.*, Memorandum Opinion and Order, 6 FCC Rcd 4387, 4387–88, para. 5 (1991) (*So. Cal. Broadcasting*).

[143] *See, e.g., Callais Cablevision, Inc.*, Notice of Apparent Liability for Monetary Forfeiture, 16 FCC Rcd 1359, 1362–63, paras. 10–11 (2001) (*Callais Cablevision*) (issuing a notice of apparent liability for forfeiture for a cable television operator's repeated signal leakage).

[144] *ADMA Telecom, Inc.*, Forfeiture Order, 26 FCC Rcd 4152, 4153–54, para. 5 (2011) (*ADMA Telecom*); *see also Callais Cablevision*, 16 FCC Rcd at 1362, para. 9; *So. Cal. Broadcasting*, 6 FCC Rcd at 4387–88, para. 5.

[145] *See* 47 U.S.C. § 503(b)(4); 47 C.F.R. § 1.80(f).

[146] *See, e.g., SBC Communications, Inc.*, Forfeiture Order, 17 FCC Rcd 7589, 7591, para. 4 (2002) (*SBC*).

A. Failure to Respond to Commission Orders

42. It is well established that a Commission licensee's failure to respond to an LOI from the Bureau violates a Commission order.[147] Such violations do not always entail a party's total failure to respond; numerous decisions recognize that parties may violate Commission orders by providing incomplete or untimely responses to Bureau LOIs or by failing to properly certify the accuracy of their responses.[148]

43. Here, as indicated above, Google persistently failed to provide declarations by individuals with personal knowledge verifying the accuracy and completeness of the Company's LOI responses. Google also failed to provide documents and information required by the Bureau's LOI. In several instances, the record reflects that Google's failure to comply with the Commission's directives was deliberate. For example, with respect to the Bureau's instruction to provide copies of all documents, including e-mail, that provided the basis for or otherwise supported Google's narrative responses to the LOI, Google initially elected, without the Bureau's consent, "not [to] undertake[] a comprehensive review of email or other communications."[149] Although a world leader in digital search capability, Google took the position that searching its employees' e-mail "would be a time-consuming and burdensome task."[150] Similarly, in response to the Bureau's directives to identify the individuals responsible for authorizing the Company's collection of Wi-Fi data, as well as any employees who had reviewed or analyzed Wi-Fi

---

[147] *See, e.g.*, *Carrera Commc'ns, LP*, Notice of Apparent Liability for Forfeiture and Order, 20 FCC Rcd 13307, 13316, para. 22 (2005) (*Carrera*) ("Carrera's willful and repeated failures to respond to the Bureau's LOIs constitute apparent violations of Commission orders."), *forfeiture issued*, Order of Forfeiture, 22 FCC Rcd 9585 (2007); *SBC*, 17 FCC Rcd at 7597–98, paras. 19–20 (interpreting the Bureau's LOI to a common carrier, which included a directive to provide a sworn statement verifying the carrier's response to the LOI, as a Commission order that the carrier was not permitted to ignore); *LDC Telecomm., Inc.*, Notice of Apparent Liability for Forfeiture and Order, 27 FCC Rcd 300, 301, para. 5 (Enf. Bur. 2012) (*LDC*) (holding that "[t]he Bureau's LOI directed to LDC was a legal order of the Commission requiring LDC to produce the requested documents and information," and that "LDC's failure to provide the documents and information sought within the time and manner specified constitute[d] a violation of a Commission order"); *Milton Goodman*, Notice of Apparent Liability for Forfeiture, 19 FCC Rcd 18119, 18121–22, paras. 4–6 (Enf. Bur. 2004) (proposing a $10,000 forfeiture based on an auction applicant's failure to respond to a Bureau LOI), *cancelled on grounds of extreme financial hardship*, Memorandum Opinion and Order, 20 FCC Rcd 658 (Enf. Bur. 2005); *see also Pendleton C. Waugh*, Opportunity to Show Cause and Notice of Opportunity for Hearing, 22 FCC Rcd 13363, 13379, para. 46 (2007) ("Under Commission precedent and Sections 4(i), 4(j), 218, 308, and 403 of the Communications Act of 1934, as amended, failure to respond appropriately to a Bureau letter of inquiry constitutes a violation of the Commission's Rules, potentially subjecting the party doing so to serious sanctions.").

[148] *See, e.g.*, *Carrera*, 20 FCC Rcd at 13319, para. 31 (proposing an $8,000 forfeiture penalty against a company not represented by counsel that filed an untimely and incomplete response to a Bureau LOI); *SBC*, 17 FCC Rcd at 7589–91, 7600, paras. 2–3, 28 (holding that a common carrier's deliberate failure to provide a sworn statement verifying its LOI response until weeks after the Bureau had directed the carrier to respond warranted a $100,000 forfeiture penalty); *Digital Antenna, Inc.*, Notice of Apparent Liability for Forfeiture and Order, 23 FCC Rcd 7600, 7600–02, paras. 3, 5, 7 (Enf. Bur. 2008) (*Digital Antenna*) (holding that a manufacturer of cellular and PCS boosters was apparently liable for violation of a Commission order when it failed to provide complete responses to Bureau LOIs, including by failing to submit the required sworn statements); *Int'l Telecom Exch.*, Order of Forfeiture, 22 FCC Rcd 13691, 13693–94, paras. 8–9 (Enf. Bur. 2007) (*ITE*) (imposing a $15,000 forfeiture penalty against a common carrier that responded to the Bureau's LOI eight months late and only after repeated requests from staff).

[149] LOI at 4; LOI Response at 1.

[150] *Id.* at 12.

communications collected by the Company, Google unilaterally determined that to do so would "serve[] no useful purpose."[151]

44. In the absence of sworn statements by individuals with personal knowledge, the Bureau was unable to rely on the completeness or accuracy of Google's responses. Moreover, the most basic aspects of any investigation are the requirements to identify persons with knowledge of the facts and to produce relevant documents. The information and documents that Google initially failed to provide included significant material. For example, one of the e-mails the Company withheld for several months recounted [redacted].

45. Obtaining the documents and information that Google should have provided in December 2010 delayed the Bureau's investigation and required considerable effort on the part of Commission staff that should not have been necessary. Google failed to provide a single e-mail in response to the LOI until April 2011—more than four months after submitting its initial LOI response.[153] Google also waited until then to identify individuals who worked on the Street View project.[154] It was not until September 2011 that Google—having received five separate demands from Commission staff—finally provided compliant declarations with respect to the accuracy and completeness of the Company's submissions.[155] Under the circumstances, Google's incomplete responses to the LOI and Supplemental LOI constitute willful and repeated violations of Commission orders.[156]

B. Proposed Forfeiture

46. Pursuant to Section 503(b)(2)(D) of the Act and Section 1.80(b)(5) of the Commission's rules, the Commission is authorized to assess a maximum forfeiture penalty of $16,000 for each violation, or each day of a continuing violation, by an entity not specifically designated in Section 503(b)(2)(A) through (C) of the Act,[157] up to a statutory maximum of $112,500 for any single continuing violation.[158] Although Section 1.80 of the Commission's rules establishes a base forfeiture amount of $4,000 for "[f]ailure to respond to Commission communications,"[159] numerous Commission decisions have departed upward from that amount when warranted under the factors outlined in Section 503(b)(2)(E) of the Act

[151] LOI at 3; LOI Response at 12.

[152] *See* Google Document 11-14.

[153] *See* Google Documents 11-7 to 11-10, 11-12 to 11-15.

[154] *See* Supplemental LOI Response at 10–12.

[155] *See* declarations attached to Sept. 2011 Response.

[156] *See, e.g.*, *Carrera*, 20 FCC Rcd at 13319, para. 31 (proposing an $8,000 forfeiture penalty against a company that filed an untimely and incomplete response to a Bureau LOI); *SBC*, 17 FCC Rcd at 7599–600, paras. 25–28 (holding that SBC's intentional failure to comply with the LOI's directive to provide a sworn statement until the Bureau issued multiple demands impeded the investigation and justified a $100,000 forfeiture); *Digital Antenna*, 23 FCC Rcd at 7600–02, paras. 3, 7 (holding that "Digital Antenna's failure to fully respond to the Bureau's inquiry"—including its failure to provide "a sworn statement or affidavit as directed in the LOI"—"constitute[d] an apparent willful and repeated violation of a Commission order" (citations omitted)).

[157] *See* 47 U.S.C. § 503(b)(2)(D); 47 C.F.R. § 1.80(b)(5).

[158] 47 C.F.R. § 1.80(b)(5).

[159] *See id.* § 1.80(b)(5) note.

and Section 1.80(b)(6) of the Commission's rules.[160] Those provisions direct the Commission (or its designee) to determine the amount of a forfeiture penalty by "tak[ing] into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[161]

47. Here, as described above, Google violated Commission orders by delaying its search for and production of responsive e-mails and other communications, by failing to identify employees, and by withholding verification of the completeness and accuracy of its submissions. Google's level of cooperation with this investigation fell well short of what we expect and require.

48. In view of the facts and circumstances apparent from the record, we find that Google's conduct warrants a substantial increase from the $4,000 base forfeiture for failure to respond to a Commission inquiry.[162] To begin with, as discussed above, there is evidence that Google's failure to cooperate with the Bureau was in many or all cases deliberate. Google refused to identify any employees or produce any e-mails in response to the Bureau's LOI. Moreover, the Company could not supply compliant declarations without identifying employees it preferred not to identify. Misconduct of this nature threatens to compromise the Commission's ability to effectively investigate possible violations of the Communications Act and the Commission's rules. Prompt and complete responses to Bureau LOIs—including sworn statements that verify the completeness and accuracy of respondents' submissions—are essential to the Commission's enforcement function.

49. An upward adjustment of the base forfeiture amount is also warranted to deter future misconduct in view of Google's ability to pay.[163] To ensure that a proposed forfeiture is not treated as simply a cost of doing business, "the Commission has determined that large or highly[ ]profitable companies . . . may be subject to proposed forfeitures that are substantially above the base forfeiture amount."[164]

---

[160] *See, e.g.*, *SBC*, 17 FCC Rcd at 7599–600, paras. 25–28 (holding that SBC's intentional failure to comply with the LOI's directive to provide a sworn statement until the Bureau issued multiple demands impeded the investigation and justified a $100,000 forfeiture); *LDC*, 27 FCC Rcd at 302, para. 8 (proposing a $25,000 forfeiture for a common carrier's apparent "egregious, intentional, and continuous" failure to respond to a Bureau LOI); *see* 47 U.S.C. § 503(b)(2)(E); 47 C.F.R. § 1.80(b)(6); *Fox Television Stations, Inc.*, Notice of Apparent Liability for Forfeiture, 25 FCC Rcd 7074, 7081, paras. 15–16 (Enf. Bur. 2010) (*Fox TV*) (proposing a $25,000 forfeiture penalty against a broadcaster that had a significant ability to pay and whose failure to respond to the Bureau's LOI "delayed [the] investigation [and] caused the Commission to expend additional, significant resources" to obtain the required information); *Digital Antenna*, 23 FCC Rcd at 7603, para. 10 (holding that Digital Antenna's incomplete LOI response, which included a failure to provide the necessary sworn verification statement, warranted an $11,000 forfeiture); *ITE*, 22 FCC Rcd at 13693–94, paras. 8–9 (imposing a $15,000 forfeiture penalty against a common carrier that responded to the Bureau's LOI eight months late and only after repeated requests from staff).

[161] 47 U.S.C. § 503(b)(2)(E); *accord* 47 C.F.R. § 1.80(b)(6).

[162] *See* 47 C.F.R. § 1.80(b)(5) note.

[163] *See* Google Inc., Annual Report (Form 10-K), at 25 (Jan. 26, 2012) (showing gross annual revenue of almost $38 billion in 2011), *available at* http://www.sec.gov/Archives/edgar/data/1288776/000119312512025336/d260164d10k.htm#toc260164_11.

[164] *Fox TV*, 25 FCC Rcd at 7081, para. 16; *see also* 47 U.S.C. § 503(b)(2)(E) (directing the Commission to take into account a violator's "ability to pay"); *accord* 47 C.F.R. § 1.80(b)(6).

50. Google's failures to identify employees, produce e-mails, and provide compliant declarations were continuing violations that lasted from December 10, 2010 until cured.[165] Accordingly, by law we may propose a forfeiture penalty of up to $112,500 for each violation.[166] Given the totality of the circumstances of this case, and our precedent in other failure to respond cases, we find that Google is apparently liable for a forfeiture penalty of $25,000.[167]

C. Section 705(a)

51. Based on its review of the evidence collected during this investigation, the Bureau has reached the following conclusions relevant to the application of Section 705(a) of the Communications Act:

- For more than two years, Google's Street View cars collected names, addresses, telephone numbers, URLs, passwords, e-mail, text messages, medical records, video and audio files, and other information from Internet users in the United States.
- The record shows that [redacted]. On at least one occasion, Engineer Doe reviewed payload data [redacted]. The Bureau was unable to determine whether Engineer Doe did anything else with the data because he declined to testify.
- The record also shows that [redacted]. The design document identified [redacted].

52. Although Google recognizes that the collection of payload data as part of its Street View project should not have happened, that does not necessarily mean the collection was unlawful. Google outlined its legal position in written submissions and in a meeting with Commission staff on May 18, 2011. The Company's position is straightforward. The Wiretap Act provides, "It shall not be unlawful under this chapter or chapter 121 of this title for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such

---

[165] *See, e.g., LDC*, 27 FCC Rcd at 302, para. 8 (characterizing LDC's failure to respond to the Bureau's LOI as "continuous"); *Net One Int'l*, Notice of Apparent Liability for Forfeiture and Order, 26 FCC Rcd 16493, 16496, para. 9 (Enf. Bur. 2011) (advising Net One that its failure "to respond fully to the LOI within ten days of the date of this NAL . . . . may constitute an additional, continuing violation"); *Resp-Org.com*, Citation, 26 FCC Rcd 3739, 3741 (Enf. Bur. 2011) ("Resp-Org.com is reminded that failure to respond to a Commission order constitutes a continuing violation."), *citation withdrawn on other grounds*, Letter, 26 FCC Rcd 8498 (Enf. Bur. 2011); *see also, e.g., ADMA Telecom*, 26 FCC Rcd at 4155, para. 8 (construing a carrier's failure to file a required document (a Form 499) with the Commission as a continuing violation until cured); *1st Source Info. Specialists, Inc.*, Notice of Apparent Liability for Forfeiture, 21 FCC Rcd 8193, 8196–97, para. 13 (2006) (characterizing a data broker's failure to respond fully to a Bureau subpoena and a citation the Bureau issued based on that failure as a continuing violation), *forfeiture issued*, Forfeiture Order, 22 FCC Rcd 431 (2007).

[166] *See* 47 C.F.R. § 1.80 (b)(5).

[167] *See, e.g., Fox TV*, 25 FCC Rcd at 7081, para. 16 (proposing a $25,000 forfeiture penalty); *ITE*, 22 FCC Rcd. at 13695, para. 13 (Enf. Bur. 2006) (imposing $15,000 forfeiture penalty for failure to respond).

electronic communication is readily accessible to the general public."[168] According to Google, the definitions of "electronic communication"[169] and "electronic communications system"[170] in the Wiretap Act plainly cover Wi-Fi communications and networks. The Wiretap Act defines "readily accessible to the general public" to mean, "with respect to a radio communication, that such communication is not . . . scrambled or encrypted."[171] Google claims that the payload data it collected was "readily accessible to the general public" because it came from unencrypted Wi-Fi networks.[172] Google further claims that the "readily accessible" exception to the Wiretap Act applies to the entirety of Section 705(a) of the Communications Act—including to the clauses prohibiting the interception or unauthorized reception of interstate radio communications—by virtue of Section 705(a)'s introductory proviso.[173] Thus, Google contends it has not violated any law within the Commission's jurisdiction to enforce.

53. After thoroughly reviewing the existing record in this investigation and applicable law, the Bureau has decided not to take enforcement action against Google for violation of Section 705(a). There is no Commission precedent addressing the application of Section 705(a) in connection with Wi-Fi communications. The available evidence, moreover, suggests that Google collected payload data only from unencrypted Wi-Fi networks, not from encrypted ones.[174] Google argues that the Wiretap Act permits the interception of unencrypted Wi-Fi communications, and some case law suggests that Section 705(a)'s prohibition on the interception or unauthorized reception of interstate radio communications excludes conduct permitted (if not expressly authorized) under the Wiretap Act.[175] Although Google also collected and stored encrypted communications sent over unencrypted Wi-Fi networks,[176] the Bureau has found no evidence that Google accessed or did anything with such encrypted communications. The Bureau's inability to compel an interview of Engineer Doe made it impossible to determine in the course of our investigation whether Google did make any use of any encrypted communications that it collected. For all these reasons, we do not find sufficient evidence that Google has violated Section 705(a) to support a finding of apparent liability under that provision in the context of this case.

V. ORDERING CLAUSES

54. Accordingly, **IT IS ORDERED** that, pursuant to Section 503(b) of the Communications Act of 1934, as amended, 47 U.S.C. § 503(b), and Section 1.80 of the Commission's rules, 47 C.F.R. § 1.80, Google Inc. is hereby **NOTIFIED** of this **APPARENT LIABILITY FOR FORFEITURE** in the amount of twenty-five thousand dollars ($25,000) for willfully and repeatedly violating an Enforcement Bureau directive to respond to a letter of inquiry.

---

[168] 18 U.S.C. § 2511(2)(g)(i).

[169] *Id.* § 2510(12).

[170] *Id.* § 2510(14).

[171] *Id.* § 2510(16)(A).

[172] *See, e.g.*, LOI Response at 2 (citing in support of that contention *United States v. Ahrndt*, No. 08-468-KI, 2010 WL 373994, at *8 (D. Or. Jan. 28, 2010)).

[173] *See supra* note 15 and accompanying text.

[174] *See supra* para. 11 (summarizing Stroz Friedberg's conclusion that Google's payload data collection was limited to unencrypted Wi-Fi networks, but also noting the limited scope of Stroz Friedberg's review).

[175] *See supra* note 15 and accompanying text.

[176] *See supra* para. 11.

55. **IT IS FURTHER ORDERED** that, pursuant to Section 1.80 of the Commission's rules, 47 C.F.R. § 1.80, within thirty (30) calendar days after the release date of this Notice of Apparent Liability for Forfeiture, Google Inc. **SHALL PAY** the full amount of the proposed forfeiture or **SHALL FILE** a written statement seeking reduction or cancellation of the proposed forfeiture.

56. Payment of the forfeiture must be made by check or similar instrument, payable to the order of the Federal Communications Commission. The payment must include the NAL/Account Number and FRN referenced above. Payment by check or money order may be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000. Payment by overnight mail may be sent to U.S. Bank – Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101. Payment by wire transfer may be made to ABA Number 021030004, receiving bank TREAS/NYC, and account number 27000001. For payment by credit card, an FCC Form 159 (Remittance Advice) must be submitted. When completing the FCC Form 159, enter the NAL/Account number in block number 23A (call sign/other ID), and enter the letters "FORF" in block number 24A (payment type code). Google Inc. will also send electronic notification to Theresa Cavanaugh at Terry.Cavanaugh@fcc.gov and Mindy Littell at Mindy.Littell@fcc.gov within forty-eight (48) hours of the date said payment is made. Requests for full payment under an installment plan should be sent to Chief Financial Officer – Financial Operations, 445 12th Street, SW, Room 1-A625, Washington, DC 20554. Please contact the Financial Operations Group Help Desk at 1-877-480-3201 or e-mail ARINQUIRIES@fcc.gov with any questions regarding payment procedures.

57. The written statement seeking reduction or cancellation of the proposed forfeiture, if any, must include a detailed factual statement supported by appropriate documentation and affidavits pursuant to Sections 1.80(f)(3) and 1.16 of the Commission's rules.[177] The written statement must be mailed both to Marlene H. Dortch, Secretary, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554, ATTN: Enforcement Bureau – Investigations and Hearings Division; and to Theresa Z. Cavanaugh, Division Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Room 4-C330, Washington, DC 20554, and must include the NAL/Acct. Number referenced in the caption. Documents sent by overnight mail (*other than* United States Postal Service Express Mail) must be addressed to Marlene H. Dortch, Secretary, Federal Communications Commission, Office of the Secretary, 9300 East Hampton Drive, Capitol Heights, MD 20743. Hand- or messenger-delivered mail should be directed, without envelopes, to Marlene H. Dortch, Secretary, Federal Communications Commission, Office of the Secretary, 445 12th Street, SW, Washington, DC 20554 (deliveries accepted Monday through Friday 8:00 a.m. to 7:00 p.m. only).[178] The Company should also send an electronic copy of any written statement to Theresa Cavanaugh at Terry.Cavanaugh@fcc.gov and Mindy Littell at Mindy.Littell@fcc.gov.

58. The Commission will not consider reducing or canceling a forfeiture in response to a claim of inability to pay unless the petitioner submits (1) federal tax returns for the most recent three-year period, (2) financial statements prepared according to generally accepted accounting practices, or (3) some other reliable and objective documentation that accurately reflects the petitioner's current financial status. Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation submitted.

59. **IT IS FURTHER ORDERED** that copies this Notice of Apparent Liability for Forfeiture shall be sent by Certified Mail Return Receipt Requested and First Class mail to Google Inc.,

[177] 47 C.F.R. §§ 1.16, 1.80(f)(3).

[178] For further instructions on FCC filing addresses, see www.fcc.gov/osec/guidelines.html.

Attention: Richard Whitt, Director/Managing Counsel, Telecom and Media Policy, 1101 New York Avenue, NW, Second Floor, Washington, DC 20005, and to E. Ashton Johnston, Counsel for Google Inc., Lampert, O'Connor & Johnston, P.C., 1776 K Street NW, Suite 700, Washington, DC 20006.

FEDERAL COMMUNICATIONS COMMISSION

P. Michele Ellison
Chief, Enforcement Bureau