Session 7: Privacy, Data and Cybersecurity

We will start by looking at a recent case regarding the extent of the Federal Trade Commission's authority in connection with a data breach, then turn to a situation regarding data collection by Google, read or watch a recent privacy talk by Apple CEO Tim Cook (text, video) and close with a speech by former FBI Director James Comey.

Federal Trade Commission v. Wyndham Worldwide Corp.

799 F.3d 236 (3rd Cir. 2015)

AMBRO, Circuit Judge. The Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a). In 2005 the Federal Trade Commission began bringing administrative actions under this provision against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. The vast majority of these cases have ended in settlement.

On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation's computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges. The FTC filed suit in federal District Court, alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham's motion to dismiss, and we granted interlocutory appeal on two issues: whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision. We affirm the District Court.

I. Background

A. Wyndham's Cybersecurity

Wyndham Worldwide is a hospitality company that franchises and manages hotels and sells timeshares through three subsidiaries. Wyndham licensed its brand name to approximately 90 independently owned hotels. Each Wyndham-branded hotel has a property management system that processes consumer information that includes names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes. Wyndham "manage[s]" these systems and requires the hotels to "purchase and configure" them to its own specifications. Compl. at ¶ 15, 17. It also operates a computer network in Phoenix, Arizona, that connects its data center with the property management systems of each of the Wyndham-branded hotels.

The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." Id. at ¶ 24. This claim is fleshed out as follows.

1. The company allowed Wyndham-branded hotels to store payment card information in clear readable text.

2. Wyndham allowed the use of easily guessed passwords to access the property management systems. For example, to gain "remote access to at least one hotel's system,"

which was developed by Micros Systems, Inc., the user ID and password were both "micros." Id. at ¶ 24(f).

3. Wyndham failed to use "readily available security measures"—such as firewalls—to "limit access between [the] hotels' property management systems, ... corporate network, and the Internet." Id. at ¶ 24(a).

4. Wyndham allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions. It did not ensure that the hotels implemented "adequate information security policies and procedures." Id. at ¶ 24(c). Also, it knowingly allowed at least one hotel to connect to the Wyndham network with an out-of-date operating system that had not received a security update in over three years. It allowed hotel servers to connect to Wyndham's network even though "default user IDs and passwords were enabled ..., which were easily available to hackers through simple Internet searches." Id.And, because it failed to maintain an "adequate[] inventory [of] computers connected to [Wyndham's] network [to] manage the devices," it was unable to identify the source of at least one of the cybersecurity attacks. Id. at ¶ 24(g).

5. Wyndham failed to "adequately restrict" the access of third-party vendors to its network and the servers of Wyndham-branded hotels. Id. at ¶ 24(j). For example, it did not "restrict[] connections to specified IP addresses or grant[] temporary, limited access, as necessary." Id.

6. It failed to employ "reasonable measures to detect and prevent unauthorized access" to its computer network or to "conduct security investigations." Id. at ¶ 24(h).

7. It did not follow "proper incident response procedures." Id. at ¶ 24(i). The hackers used similar methods in each attack, and yet Wyndham failed to monitor its network for malware used in the previous intrusions.

Although not before us on appeal, the complaint also raises a deception claim, alleging that since 2008 Wyndham has published a privacy policy on its website that overstates the company's cybersecurity.

> We safeguard our Customers' personally identifiable information by using industry standard practices. Although "guaranteed security" does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such [i]nformation consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for encrypting data. This protects confidential information—such as credit card numbers, online forms, and financial data—from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain "fire walls" and other appropriate safeguards....

Id. at ¶ 21. The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data.

B. The Three Cybersecurity Attacks

As noted, on three occasions in 2008 and 2009 hackers accessed Wyndham's network and the property management systems of Wyndham-branded hotels. In April 2008, hackers first broke into the local network of a hotel in Phoenix, Arizona, which was connected to Wyndham's network and the Internet. They then used the brute-force method—repeatedly guessing users' login IDs and passwords—to access an administrator account on Wyndham's network. This enabled them to obtain consumer data on computers throughout the network. In total, the hackers obtained unencrypted information for over 500,000 accounts, which they sent to a domain in Russia.

In March 2009, hackers attacked again, this time by accessing Wyndham's network through an administrative account. The FTC claims that Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges. Wyndham then discovered "memory-scraping malware" used in the previous attack on more than thirty hotels' computer systems. Id. at ¶ 34. The FTC asserts that, due to Wyndham's "failure to monitor [the network] for the malware used in the previous attack, hackers had unauthorized access to [its] network for approximately two months." Id. In this second attack, the hackers obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels.

Hackers in late 2009 breached Wyndham's cybersecurity a third time by accessing an administrator account on one of its networks. Because Wyndham "had still not adequately limited access between... the Wyndham-branded hotels' property management systems, [Wyndham's network], and the Internet," the hackers had access to the property management servers of multiple hotels. Id. at ¶ 37. Wyndham only learned of the intrusion in January 2010 when a credit card company received complaints from cardholders. In this third attack, hackers obtained payment card information for approximately 69,000 customers from the property management systems of 28 hotels.

The FTC alleges that, in total, the hackers obtained payment card information from over 619,000 consumers, which (as noted) resulted in at least $10.6 million in fraud loss. It further states that consumers suffered financial injury through "unreimbursed fraudulent charges, increased costs, and lost access to funds or credit," Id. at ¶ 40, and that they "expended time and money resolving fraudulent charges and mitigating subsequent harm." Id.
***

III. FTC's Regulatory Authority Under § 45(a)

A. Legal Background

The Federal Trade Commission Act of 1914 prohibited "unfair methods of competition in commerce." Pub.L. No. 63-203, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § 45(a)). *** After several early cases limited "unfair methods of competition" to practices harming competitors and not consumers, see, e.g., *FTC v. Raladam Co.*, 283 U.S. 643 (1931), Congress inserted an additional prohibition in § 45(a) against "unfair or deceptive acts or practices in or affecting commerce," Wheeler-Lea Act, Pub.L. No. 75-447, § 5, 52 Stat. 111, 111 (1938).

For the next few decades, the FTC interpreted the unfair-practices prong primarily through agency adjudication. But in 1964 it issued a "Statement of Basis and Purpose" for

unfair or deceptive advertising and labeling of cigarettes, 29 Fed.Reg. 8324, 8355 (July 2, 1964), which explained that the following three factors governed unfairness determinations:

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers (or competitors or other businessmen).

Id.

In 1994, Congress codified the 1980 Policy Statement at 15 U.S.C. § 45(n):

> The Commission shall have no authority under this section ... to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

FTC Act Amendments of 1994, Pub.L. No. 103-312, § 9, 108 Stat. 1691, 1695. Like the 1980 Policy Statement, § 45(n) requires substantial injury that is not reasonably avoidable by consumers and that is not outweighed by the benefits to consumers or competition. It also acknowledges the potential significance of public policy and does not expressly require that an unfair practice be immoral, unethical, unscrupulous, or oppressive.

B. Plain Meaning of Unfairness

Wyndham argues (for the first time on appeal) that the three requirements of 15 U.S.C. § 45(n) are necessary but insufficient conditions of an unfair practice and that the plain meaning of the word "unfair" imposes independent requirements that are not met here. Arguably, § 45(n) may not identify all of the requirements for an unfairness claim. (While the provision forbids the FTC from declaring an act unfair "unless" the act satisfies the three specified requirements, it does not answer whether these are the *only* requirements for a finding of unfairness.) Even if so, some of Wyndham's proposed requirements are unpersuasive, and the rest are satisfied by the allegations in the FTC's complaint.

First, citing *FTC v. R.F. Keppel & Brother, Inc.*, 291 U.S. 304 (1934), Wyndham argues that conduct is only unfair when it injures consumers "through unscrupulous or unethical behavior." Wyndham Br. at 20-21. But *Keppel* nowhere says that unfair conduct must be unscrupulous or unethical. Moreover, in *Sperry* the Supreme Court rejected the view that the FTC's 1964 policy statement required unfair conduct to be "unscrupulous" or "unethical." 405 U.S. at 244 n. 5. Wyndham points to no subsequent FTC policy statements, adjudications, judicial opinions, or statutes that would suggest any change since Sperry.

Next, citing one dictionary, Wyndham argues that a practice is only "unfair" if it is "not equitable" or is "marked by injustice, partiality, or deception." Wyndham Br. at 18-19 (citing *Webster's Ninth New Collegiate Dictionary* (1988)). Whether these are requirements of an unfairness claim makes little difference here. A company does not act equitably when it

publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.

*** Continuing on, Wyndham asserts that a business "does not treat its customers in an 'unfair' manner when the business itself is victimized by criminals." Wyndham Br. at 21 (emphasis in original). It offers no reasoning or authority for this principle, and we can think of none ourselves. *** We are therefore not persuaded by Wyndham's arguments that the alleged conduct falls outside the plain meaning of "unfair." *** Having rejected Wyndham's arguments that its conduct cannot be unfair, we assume for the remainder of this opinion that it was.

IV. Fair Notice

A conviction or punishment violates the Due Process Clause of our Constitution if the statute or regulation under which it is obtained "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *FCC v. Fox Television Stations, Inc.*, ___ U.S. ___ (2012) (internal quotation marks omitted). Wyndham claims that, notwithstanding whether its conduct was unfair under § 45(a), the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow. ***

We thus conclude that Wyndham was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by § 45(a). Instead, the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute. If later proceedings in this case develop such that the proper resolution is to defer to an agency interpretation that gives rise to Wyndham's liability, we leave to that time a fuller exploration of the level of notice required. For now, however, it is enough to say that we accept Wyndham's forceful contention that we are interpreting the FTC Act (as the District Court did). As a necessary consequence, Wyndham is only entitled to notice of the meaning of the statute and not to the agency's interpretation of the statute.

B. Did Wyndham Have Fair Notice of the Meaning of § 45(a)?

Having decided that Wyndham is entitled to notice of the meaning of the statute, we next consider whether the case should be dismissed based on fair notice principles. We do not read Wyndham's briefs as arguing the company lacked fair notice that cybersecurity practices can, as a general matter, form the basis of an unfair practice under § 45(a). Wyndham argues instead it lacked notice of what *specific* cybersecurity practices are necessary to avoid liability. We have little trouble rejecting this claim. *** In sum, we have little trouble rejecting Wyndham's fair notice claim.

V. Conclusion

The three requirements in § 45(n) may be necessary rather than sufficient conditions of an unfair practice, but we are not persuaded that any other requirements proposed by Wyndham pose a serious challenge to the FTC's claim here. Furthermore, Wyndham repeatedly argued there is no FTC interpretation of § 45(a) or (n) to which the federal courts must

defer in this case, and, as a result, the courts must interpret the meaning of the statute as it applies to Wyndham's conduct in the first instance. Thus, Wyndham cannot argue it was entitled to know with ascertainable certainty the cybersecurity standards by which the FTC expected it to conform. Instead, the company can only claim that it lacked fair notice of the meaning of the statute itself—a theory it did not meaningfully raise and that we strongly suspect would be unpersuasive under the facts of this case.

We thus affirm the District Court's decision.

STATEMENT OF THE COMMISSION

United States of America v. Google Inc.
(United States District Court for the Northern District of California)
In the Matter of Google Inc., FTC Docket No. C-4336

August 9, 2012

The Federal Trade Commission has approved a proposed federal court consent order imposing a $22.5 million civil penalty on Google Inc., the highest fine ever levied for violation of a Commission consent order.[1] That the violations alleged in the Commission's federal court complaint have warranted so significant a penalty signals to Google and other companies that the Commission will vigorously enforce its orders.

We write to respond to our colleague, Commissioner Rosch, who opposes approval of the settlement with Google because it includes a denial of the substantive allegations in the Commission's civil penalty complaint.[2] While Commissioner Rosch agrees that the Commission has the requisite "reason to believe" that Google violated the underlying FTC consent order, he does not believe that the settlement is in the public interest because Google denies the FTC's allegations.[3] Commissioner Rosch takes issue with the Commission permitting Google to deny liability in the consent order while at the same time approving a civil penalty of $22.5 million against the company.

We strongly disagree with Commissioner Rosch's view that if the Commission allows a defendant to deny the complaint's substantive allegations, the settlement is not in the public interest. Here, as in all cases, a defendant's denial of liability in a settlement agreement has no bearing on the Commission's determination as to whether it has reason to believe the defendant has violated the law or that a proposed settlement will afford appropriate relief for the Commission's charges. To the contrary, the Commission acts based on its consideration of the staff's investigative work, and in this instance we have strong reason to believe that Google violated its order. The FTC staff's careful investigation in this case clearly demonstrated that the historic $22.5 million fine is an appropriate remedy for our charge that Google violated a Commission order by misrepresenting to Safari browser users how to avoid targeted advertising by Google.

Nor is a denial of liability inconsistent with the imposition of a civil penalty.[4] This is a settlement, and, in our view, the most important question is whether Google will abide by the

---

[1] The Commission consent order against Google became effective on October 28, 2011.

[2] The order states that Google "denies any violation of the FTC Order, any and all liability for the claims set forth in the Complaint, and all material allegations of the Complaint save for those regarding jurisdiction and venue." Order, Stipulated Fact 2.

[3] Dissenting Statement of Commissioner Rosch at 1.

[4] *See, e.g., United States v. ChoicePoint, Inc.*, No. 1:06-cv-0198 (N.D. Ga. Feb. 15, 2006) (Stipulated Final Judgment and Order) (defendant expressly denied liability in consent order imposing then-largest FTC civil penalty); *see also United States v. ChoicePoint, Inc.*, No. 1:06-cv-0198 (N.D. Ga. Oct. 14, 2009) (Supplemental

underlying FTC consent order going forward.[5] We firmly believe that the Commission's swift imposition of a $22.5 million fine helps to promote such future compliance. With a company of Google's size, almost any penalty can be dismissed as insufficient.[6] But it is hardly inconsequential to impose a $22.5 million civil penalty when the accompanying complaint does not allege that the conduct at issue yielded significant revenue or endured for a significant period of time. This settlement is intended to provide a strong message to Google and other companies under order that their actions will be under close scrutiny and that the Commission will respond to violations quickly and vigorously.

Stipulated Judgment and Order) (contempt settlement in which defendant expressly denied liability for FTC order violations).

[5] *Cf. United States v. Microsoft Corp.*, 56 F.3d 1448, 1461 (D.C. Cir. 1995) ("The important question is whether Microsoft will abide by the terms of the consent decree regardless of whether it is willing to admit wrongdoing.").

[6] *See* Dissenting Statement of Commissioner Rosch at 2.

STUART DELERY
Acting Assistant Attorney General, Civil Division

MELINDA HAAG (CABN 132612)
United States Attorney for the Northern District of California

MAAME EWUSI-MENSAH FRIMPONG (CABN 222986)
Deputy Assistant Attorney General, Civil Division

MICHAEL S. BLUME (PA 78525)
Director, Consumer Protection Branch

ADRIENNE E. FOWLER*
Trial Attorney, Consumer Protection Branch, U.S. Department of Justice
450 5th St. NW, Room 6400
Washington, DC 20530
(202) 514-9471
(202) 514-8742 (fax)
Adrienne.E.Fowler@usdoj.gov

Attorneys for the United States

Fee exempt
(99)

ADR

E-filing

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. GOOGLE INC. Defendant.	Case No. CV 12-04177 HRL **COMPLAINT FOR CIVIL PENALTIES AND OTHER RELIEF**

Plaintiff, the United States of America, acting upon the notification and authorization to the Attorney General by the Federal Trade Commission ("FTC" or "Commission"), for its Complaint alleges that:

* Member in good standing of the New York Bar, which does not issue bar numbers.

1. Plaintiff brings this action under Sections 5(*l*) and 16(a) of the Federal Trade Commission Act as amended ("FTC Act"), 15 U.S.C. §§ 45(*l*) and 56(a), to obtain monetary civil penalties and other relief for Defendant's violations of a final Commission order.

JURISDICTION

2. This Court has jurisdiction over this matter pursuant to 28 U.S.C. §§ 1331, 1337(a), 1345, and 1355, and 15 U.S.C. §§ 45(*l*) and 56(a).

VENUE

3. Venue in this district is proper under 28 U.S.C. §§ 1391(b)-(c) and 1395(a).

DEFENDANT

4. Defendant Google Inc. ("Google") is a Delaware corporation with its principal office or place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043. At all times material to this Complaint, Defendant has participated in the acts and practices described in this Complaint. Defendant transacts business in this district.

COMMERCE

5. At all times material to this Complaint, Defendant has maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

PRIOR COMMISSION PROCEEDING

6. In an administrative proceeding bearing Docket No. C-4336, the Commission charged Google with violating the FTC Act in connection with Google's launch of its social networking tool, Google Buzz.

7. The FTC alleged, among other things, that Google misrepresented to users of its Gmail email service that: (1) Google would not use their information for any purpose other than to provide that email service; (2) users would not be automatically enrolled in the Buzz network; and (3) users could control what information would be public on their Buzz profiles.

8. On October 13, 2011, the Commission entered its decision and order ("Google Consent Order") approving a settlement with Google. The Google Consent Order contains the following prohibitions:

> I.
>
> IT IS ORDERED that respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:
>
> A. the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.
>
> B. the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other entity, including, but not limited to, the U.S.-EU Safe Harbor.

9. The Google Consent Order defines "covered information" as:

> information Google collects from or about an individual, including, but not limited to, an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.

10. Covered information as defined under the Google Consent Order includes a persistent identifier contained in a tracking cookie, a user's IP address, a user's account ID, a user's interests, or a user's web-browsing activity.

11. The FTC served the Google Consent Order on Google on October 28, 2011, and it remains in full force. A copy of the Google Consent Order is attached as Exhibit A.

DEFENDANT'S BUSINESS PRACTICES

12. This Complaint alleges (as detailed below) that Google represented to certain users that Google would not place tracking cookies or serve targeted advertisements based on

those tracking cookies—but those users did in fact receive tracking cookies and targeted advertisements.

13. Google is a global technology company best known for its online search engine, which provides free search results to users. Google also provides free web products to consumers, including its widely used web-based email service, Gmail.

14. In exchange for fees, Google provides advertising services to online advertisers and publishers. Through its various advertising networks, Google allows advertisers to deliver targeted advertisements to users. Through Google, advertisers serve *billions* of online advertisements every single day. In 2011, Google received $36.5 billion from advertising fees, of which approximately $1.7 billion came from online display ads. Indeed, in 2011, 96% of Google's revenue came from online advertising, according to Google's filings with the Securities and Exchange Commission.

15. Google is a member of the Network Advertising Initiative ("NAI"), a self-regulatory organization for companies in the online advertising marketplace. As an NAI member, Google must adhere to NAI's Self-Regulatory Code of Conduct ("NAI Code"). Section III(2)(a) of the NAI Code provides:

> Each member directly engaging in online behavioral advertising, multi-site advertising, and/or ad delivery and reporting shall clearly and conspicuously post notice on its website that describes its data collection, transfer, and use practices. Such notice shall include[:]
>
> i. The online behavioral advertising, multi-site advertising, and/or ad delivery and reporting activities undertaken by the member company;
>
> ii. What types of data are collected by the member company; [and]
>
> iii. How such data will be used by the member company, including transfer, if any, of data to a third party[.]

16. Google has stated, including on its Privacy Policy for Ads and Advertising Services webpage, that it is a member of NAI. Google has also authorized other entities,

including NAI, to represent that it is a participating NAI member that complies with NAI's Code.

Targeted Advertising

17. Targeted advertising uses information collected from a user's web-browsing activity, such as past or present search queries or websites a user visits or has visited, to serve online advertisements tailored to the individual user.

18. Targeted advertising often utilizes HTTP cookies, which are small text files that can be used to collect and store information about a user's online activities, such as the content and advertisements a user viewed or the webpages he or she visited ("tracking cookies"). These cookies contain a unique persistent identifier that allows an advertising network to recognize the user's computer and correlate the user's web-browsing activity with the computer.

19. Tracking cookies are placed, or "set," by either first parties or third parties. First-party cookies are placed by the website the user is visiting. For example, if a user visits <www.google.com>, any cookie that Google sets from that same domain <google.com> while the user is visiting that website is a first-party cookie. First-party cookies are often used to help websites remember certain information about a user, such as items in a shopping cart, a log-in name, or the user's preferences.

20. Third-party cookies are placed by a domain other than the one the user is visiting. For example, if a user visits <www.google.com>, a cookie placed from any domain other than <google.com> is a third-party cookie. Third-party cookies are usually set by an advertising network or a company that serves content on the website a user is visiting, such as a banner ad.

21. An advertising network may set tracking cookies in either the third-party or first-party context. For instance, if a user clicks on an advertisement, the advertising network may set a first-party tracking cookie on the user's browser. An advertising network can place a third-party tracking cookie when a user merely visits a website where the network displays an ad.

22. By placing a tracking cookie on a user's browser, an advertising network may collect information about the user's web-browsing activities and use that information to serve online advertisements that are targeted to the user's predicted interests.

Defendant's DoubleClick Advertising Cookie

23. Google uses the "DoubleClick Advertising Cookie" to collect information and serve targeted advertisements to users who visit Google websites, Google partner websites, and websites that use Google's advertising services.

24. Notably, Google sets the DoubleClick Advertising Cookie on the user's computer from the <doubleclick.net> domain. Therefore, when a user visits a website on a domain other than <doubleclick.net>, a cookie set from <doubleclick.net> is a third-party cookie. But when a user clicks on a DoubleClick advertisement, a cookie set from <doubleclick.net> is a first-party cookie.

25. Through each DoubleClick Advertising Cookie, Google assigns a unique persistent identifier to a user, which enables Google to collect and use information about that user, including the user's IP address and web-browsing activity. Through each cookie's unique persistent identifier, Google can track that user's activity and Google's advertising network can link the user's web-browsing activity to the computer over time.

26. Based on the information Google collects via the DoubleClick Advertising Cookie, Google creates predicted interest categories for a user and considers what advertising is most likely to appeal to that user. Once Google has linked interest categories with a particular user's computer, Google uses the cookie's unique persistent identifier to serve targeted advertisements tailored to the user's predicted interests during his or her online activity.

Safari Browser Privacy Controls

27. Web browsers provide users with different ways to delete, block, or limit cookies set on their browser.

28. Through a web browser's privacy settings, users can choose to categorically block or accept all cookies, or to block cookies from particular websites or domains. Certain browsers

allow users to block all third-party cookies.

29. Apple's Safari browser blocks third-party cookies by default. Apple advertises this default setting as a benefit of choosing Safari. Specifically, Apple states: "Some companies track the cookies generated by the websites you visit, so they can gather and sell information about your web activity. Safari is the first browser that blocks these tracking cookies by default, better protecting your privacy."

30. The Safari browser, however, allows third-party cookies in certain exceptional circumstances. In particular, it permits third-party cookies if a user submits information via a form embedded within the webpage, known as a "form submission." For example, when a user submits information through a website (such as typing a mailing address to make an online purchase or filling out an online customer survey), that website may seek to set third-party cookies on the user's browser. In such cases, the Safari browser accepts third-party cookies.

31. Significantly, the Safari browser's default setting blocks third-party cookies *only* from a *new* domain. Once the Safari browser accepts (and retains) a cookie, Safari will allow *any* additional cookies from that same domain. In other words, once Safari allows a cookie from the <doubleclick.net> domain, it will allow any additional cookies from <doubleclick.net>.

Defendant's Advertising Privacy Controls

32. Since entering the online advertising market, Google has acknowledged that some users would be wary of targeted advertising. Google therefore permits users who do not want their information collected or used for the delivery of targeted advertising to "opt out."

33. A user may opt out of targeted advertising either by clicking a button on Google's Ads Preferences webpage ("opt-out button") or by downloading Google's "advertising cookie opt-out plugin." Both of these options place an "opt-out cookie" on the user's browser. (Google uses the term "opt-out cookie" interchangeably with the term "the DoubleClick opt-out cookie.")

34. The opt-out button saves the opt-out cookie temporarily on a user's browser until the user clears or deletes the browser's cookies. The plugin saves the opt-out cookie

permanently on a user's browser, so that if a user deletes or clears the browser's cookies, the opt-out cookie will remain.

35. Google gives users of three browsers (Internet Explorer, Firefox, and Google Chrome) the ability to download the plugin. For technical reasons, Google does not offer the plugin to users of the Safari browser.

DEFENDANT'S STATEMENTS

36. However, Google told Safari users that they did not need to take any action to be opted out of DoubleClick targeted advertisements.

37. Google assured Safari users that the Safari default setting "effectively accomplishes the same thing as setting the opt-out cookie," as shown in the highlighted portions of the Google webpage for the Advertising Cookie Opt-out Plugin (highlighting added for emphasis):

Google **Advertising Cookie Opt-out Plugin**

Home
FAQs
Browser instructions

Opting out permanently: Browser Instructions

See instructions for: Internet Explorer, Firefox & Google Chrome | Safari | Other browsers

Internet Explorer, Mozilla Firefox & Google Chrome

You can download the plugin for Internet Explorer, for Firefox and for Google Chrome from the homepage of the Google advertising opt-out plugin.

Instructions for Safari

While we don't yet have a Safari version of the Google advertising cookie opt-out plugin, Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the opt-out cookie. To confirm that Safari is set up to block third-party cookies, do the following:

1. From Safari, select "Safari" in the menu bar, and then select "Preferences"
2. In the Preferences Dialog Box, select the "Security" tab
3. Make sure the "Accept cookies:" setting is set to "Only from sites you navigate to". You can also set this option to "Never", but this will prevent many web sites that rely on cookies from working.

Instructions for other browsers

Unfortunately, the plugin is not available for other browsers. You can always opt out using the Ads Preferences Manager, but without a special browser plugin, your opt-out setting will go away when you delete your browser's cookies (you would need to set it again manually).

If you're using another browser that's not mentioned above, you can look for a common feature, which accomplishes the same as setting the DoubleClick opt-out cookie: Find a setting in your browser's settings that allows you to only accept cookies from sites you visit, or only "first-party cookies". This option may also be described as "blocking third-party cookies."

©2010 Google - Home - Privacy Policy

38. Google made further assurances to all users (including Safari users), as follows:

A. On its Advertising and Privacy page, Google states: "After you opt out, Google will not collect interest category information and you will not receive interest-based ads."

B. On its Privacy Policy for Google Ads and Advertising Services page, Google stated:

> If you select the DoubleClick opt-out cookie, ads delivered to your browser by our ad-serving technology will not be served based on the DoubleClick cookie. Your DoubleClick opt-out cookie will not be uniquely identified . . . . As long as your browser retains the DoubleClick opt-out cookie, Google won't serve new DoubleClick cookies to your browser.

39. Notably, Google's statements in Paragraph 38 applied with equal force to first-party and third-party cookies.

40. Thus, Google represented to Safari users that, if they did not change the default setting, Google would not place DoubleClick Advertising Cookies on a user's browser, collect interest category information from or about the user, or serve targeted advertisements to the user.

DEFENDANT'S CONDUCT

41. Despite its representations to Safari users, Google overrode the Safari default browser setting and placed the DoubleClick Advertising Cookie on Safari browsers.

42. Specifically, when a Safari user with the default browser setting visited a Google website, Google partner website, or website that used Google's advertising services, Google used code that was invisible to the user to communicate with that user's Safari browser. That communication stated, unbeknownst to the user, that the user was generating a "form submission." In reality, Google was setting a cookie on the user's browser (the "Initial Cookie").

43. As a direct result of that "form submission," the Safari browser accepted the Initial Cookie.

44. The Initial Cookie enables Google to store, collect, and transmit, in encrypted form, a user's Google Account ID.

45. Google set the Initial Cookie from the <doubleclick.net> domain, the same domain that Google uses to serve the DoubleClick Advertising Cookie.

46. After the Safari browser accepted the Initial Cookie, Google set additional third-party cookies (including but not limited to the DoubleClick Advertising Cookie) onto the user's browser.

47. Alternatively, Google set the DoubleClick Advertising Cookie as a first-party cookie on Safari browsers with the default setting whenever those Safari users clicked on a DoubleClick advertisement. In contrast, for users of other browsers (such as Internet Explorer, Firefox, and Chrome) who had opted out of targeted advertising, Google did not set the DoubleClick Advertising Cookie as a first-party cookie when those users clicked on a DoubleClick advertisement.

48. Setting these cookies onto users' Safari browsers enabled Google to collect information about, and serve targeted advertisements to, these users.

FIRST CAUSE OF ACTION

(Collecting Covered Information)

49. Through the statements on its website referred to in Paragraphs 37-40, including but not necessarily limited to those materials attached as Exhibit B, Defendant represented to Safari users, directly or by implication, that it would not place DoubleClick Advertising Cookies on the browsers of Safari users who had not changed the default browser setting, or collect or use information from or about users' web-browsing activity, including interest category information, from Safari users who had not changed the default browser setting.

50. In truth and in fact, Defendant placed DoubleClick Advertising Cookies on the browsers of Safari users with the default setting and to whom Google made the representations referred to in Paragraph 49, and Defendant collected and used information from or about users' web-browsing activity, including interest category information, from Safari users with the default setting and to whom Google made the representations referred to in Paragraph 49.

51. Based on the facts described in Paragraphs 49-50, Defendant misrepresented the extent to which users may exercise control over the collection or use of covered information, thereby violating Part I(A) of the Google Consent Order.

SECOND CAUSE OF ACTION

(Serving Targeted Advertisements)

52. Through the statements on its website referred to in Paragraphs 37-40, including but not necessarily limited to those materials attached as Exhibit B, Defendant represented to Safari users, directly or by implication, that it would not serve targeted advertisements based on information collected via the DoubleClick Advertising Cookie to Safari users who had not changed their default browser setting.

53. In truth and in fact, Defendant did serve targeted advertisements based on information collected via the DoubleClick Advertising Cookie to Safari users with the default setting and to whom Google made the representations referred to in Paragraph 52.

54. Based on the facts described in Paragraphs 52-53, Defendant misrepresented the extent to which users may exercise control over the collection or use of covered information, thereby violating Part I(A) of the Google Consent Order.

THIRD CAUSE OF ACTION

(Misrepresenting NAI Code Compliance)

55. Through the statements on its website referred to in Paragraph 16, including but not necessarily limited to those materials attached as Exhibit B, Defendant represented, directly or by implication, that it adheres to or complies with the NAI Code, which is a privacy, security, or compliance program that requires Defendant to disclose its data collection and use practices.

56. In truth and in fact, Defendant did not disclose the data collection and use practices described in Paragraphs 41-48, thereby violating Section III(2)(a) of the NAI Code referred to in Paragraph 15.

57. Based on the facts described in Paragraphs 55-56, Defendant misrepresented the

extent to which it adheres to or complies with a privacy, security, or compliance program, thereby violating Part I(B) of the Google Consent Order.

CIVIL PENALTIES

58. Each misrepresentation to Safari users by Google that it would not place the DoubleClick Advertising Cookie or collect or use interest category information, in violation of the Google Consent Order, as described above, constitutes a separate violation for which Plaintiff seeks monetary civil penalties.

59. Each misrepresentation to Safari users by Google that it would not serve targeted ads based on information collected via the DoubleClick Advertising Cookie, in violation of the Google Consent Order, as described above, constitutes a separate violation for which Plaintiff seeks monetary civil penalties.

60. Each misrepresentation by Google that it adhered to or complied with the NAI Code, in violation of the Google Consent Order, as described above, constitutes a separate violation for which Plaintiff seeks monetary civil penalties.

61. Section 5(*l*) of the FTC Act, 15 U.S.C. § 45(*l*), as modified by Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461, and Section 1.98(c) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(c), authorizes the Court to award monetary civil penalties of not more than $16,000 for each such violation of the Google Consent Order.

62. Under Sections 5(*l*) and 13(b) of the FTC Act, 15 U.S.C. §§ 45(*l*) and 53(b), this Court is authorized to permanently enjoin Defendant from violating the Google Consent Order as well as to grant ancillary relief.

PRAYER FOR RELIEF

63. WHEREFORE, Plaintiff requests this Court, pursuant to 15 U.S.C. §§ 45(*l*) and 56(a), and pursuant to the Court's own equitable powers to:

(1) Enter judgment against Defendant and in favor of the Plaintiff for each violation of the Google Consent Order alleged in this Complaint;

(2) Award Plaintiff monetary civil penalties from Defendant for each violation of the Google Consent Order alleged in this Complaint;

(3) Enjoin Defendant from violating the Google Consent Order issued in Docket No. C-4336;

(4) Award Plaintiff its costs and attorneys' fees incurred in connection with this action; and

(5) Award Plaintiff such additional relief as the Court may deem just and proper.

Date: Aug. 8, 2012

Of Counsel:

JAMES A. KOHM
Associate Director for Enforcement

LAURA KIM
Assistant Director for Enforcement

MEGAN E. GRAY
Attorney
MEGAN A. BARTLEY
Attorney
Federal Trade Commission
Bureau of Consumer Protection
Division of Enforcement
600 Pennsylvania Avenue, N.W.
Mail Drop M-8102B
Washington, DC 20580
(202) 326-3408, mgray@ftc.gov
(202) 326-3424, mbartley@ftc.gov
(202) 326-2558 (fax)

Respectfully submitted:

STUART F. DELERY
Acting Assistant Attorney General,
Civil Division

MELINDA HAAG (CABN 132612)
United States Attorney
for the Northern District of California

MAAME EWUSI-MENSAH FRIMPONG
(CABN 222986)
Deputy Assistant Attorney General, Civil Division

MICHAEL S. BLUME (PA 78525)
Director, Consumer Protection Branch

ADRIENNE E. FOWLER (member in good standing of the New York bar)
Trial Attorney
Consumer Protection Branch
Department of Justice, Civil Division
450 5th St. NW, Suite 6400
Washington, DC 20530
(202) 514-9471
(202) 514-8742 (fax)
Adrienne.E.Fowler@usdoj.gov

Exhibit A

102 3136

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of	)	
	)	**DOCKET NO. C-4336**
GOOGLE INC.,	)	
a corporation.	)	

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft of Complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act; and

The Respondent and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of the agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such complaint, or that any of the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Google is a Delaware corporation with its principal office or place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, "respondent" shall mean Google, its successors and assigns, officers, agents, representatives, and employees. For the purpose of Parts I, II, and III of this order, "respondent" shall also mean Google acting directly or through any corporation, subsidiary, division, website, or other device.

2. "Clear(ly) and prominent(ly)" shall mean:

   A. In textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;

   B. In communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;

   C. In communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subpart (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and

   D. In all instances, the required disclosures: (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any other statements or disclosures provided by respondent.

3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

4. "Google user" shall mean an identified individual from whom respondent has collected information for the purpose of providing access to respondent's products and services.

5. "Covered information" shall mean information respondent collects from or about an individual, including, but not limited to, an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.

6. "Third party" shall mean any individual or entity other than: (1) respondent; (2) a service provider of respondent that: (i) uses or receives covered information collected by or on behalf of respondent for and at the direction of the respondent and no other individual or entity, (ii) does not disclose the data, or any individually identifiable information derived from such data, to any individual or entity other than respondent, and (iii) does not use the data for any other purpose; or (3) any entity that uses covered information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce respondent's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

I.

IT IS ORDERED that respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

A. the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.

B. the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other entity, including, but not limited to, the U.S.-EU Safe Harbor Framework.

II.

IT IS FURTHER ORDERED that respondent, prior to any new or additional sharing by respondent of the Google user's identified information with any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, shall:

A. Separate and apart from any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, clearly and prominently disclose: (1) that the Google user's information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for respondent's sharing; and

B. Obtain express affirmative consent from the Google user to such sharing.

III.

IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent's unauthorized collection, use, or disclosure of covered information, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

C. the design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those privacy controls and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate privacy protections.

E. the evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any

other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with Part III of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons conducting such Assessments and preparing such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific privacy controls that respondent has implemented and maintained during the reporting period;

B. explain how such privacy controls are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information;

C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part III of this order; and

D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

V.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, unless respondent asserts a valid legal privilege, a print or electronic copy of:

A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements that describe the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, with all materials relied upon in making or disseminating such statements;

B. for a period of six (6) months from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that allege unauthorized collection, use, or disclosure of covered information and any responses to such complaints;

C. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

D. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director,

Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VIII.

IT IS FURTHER ORDERED that respondent shall, within ninety (90) days after the date of service of this order file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form in which respondent has complied with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate written reports.

IX.

This order will terminate on October 13, 2031, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in fewer than twenty (20) years;

B. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: October 13, 2011

Exhibit B

Google **Advertising Cookie Opt-out Plugin**

Home
FAQs
Browser instructions

Opting out permanently: Browser Instructions

See instructions for: Internet Explorer, Firefox & Google Chrome | Safari | Other browsers

Internet Explorer, Mozilla Firefox & Google Chrome

You can download the plugin for Internet Explorer, for Firefox and for Google Chrome from the homepage of the Google advertising opt-out plugin.

Instructions for Safari

While we don't yet have a Safari version of the Google advertising cookie opt-out plugin, Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the opt-out cookie. To confirm that Safari is set up to block third-party cookies, do the following:

1. From Safari, select "Safari" in the menu bar, and then select "Preferences"
2. In the Preferences Dialog Box, select the "Security" tab
3. Make sure the "Accept cookies:" setting is set to "Only from sites you navigate to". You can also set this option to "Never", but this will prevent many web sites that rely on cookies from working.

Instructions for other browsers

Unfortunately, the plugin is not available for other browsers. You can always opt out using the Ads Preferences Manager, but without a special browser plugin, your opt-out setting will go away when you delete your browser's cookies (you would need to set it again manually).

If you're using another browser that's not mentioned above, you can look for a common feature, which accomplishes the same as setting the DoubleClick opt-out cookie: Find a setting in your browser's settings that allows you to only accept cookies from sites you visit, or only "first-party cookies". This option may also be described as "blocking third-party cookies."

categories that are relevant to you. Using the Ads Preferences Manager for browsers and Ads Preferences Manager App for applications, you can remove any interest categories that don't apply and Google will no longer use them for showing you interest-based ads. You can also change which demographic categories are associated with your browser or anonymous ID. When you edit your ads preferences, your new settings may not take immediate effect, since it takes time for the change to be processed in our systems.

How do I opt out of interest-based advertising?

If you prefer not to receive interest-based advertising in web browsers, you can always click on the "Opt out" button on the Ads Preferences Manager. When you are accessing the web through a web browser, Google also offers a number of options to permanently save your opt-out settings in your browser. After you opt out, Google will not collect interest category information and you will not receive interest-based ads. You will still see the same number of ads as before, and Google may still show relevant ads based on the content of a web page, or other non-personal information. For example, if you visit a gardening site, Google can determine the content of the site and may automatically show ads related to gardening to all visitors without using a cookie. Additionally, whenever we serve an ad on Google search or on the sites of our AdSense for search partners, the ads which are displayed may still be based on the search terms you enter.

If you prefer not to receive interest-based advertising in applications and other clients that use an anonymous ID, you can always opt out using the appropriate preferences manager.

Read more about opting-out of interest-based advertising in applications and other clients.

What is the Ads Preferences Manager?

The Ads Preferences Manager is a Google site where you can manage settings associated with the ads you see. Our goal is to provide you with transparency and choice about the ads we show you.

- For Google search and Gmail, we explain why you got specific ads, and we also let you block ads from websites you aren't interested in.
- For websites that have partnered with Google to show AdWords ads, we show you a list of interests we associate with you that can affect the ads you see on those websites. We also let you add or delete interests from that list.

How does Google use cookies to serve ads?

A cookie is a snippet of text that is sent from a website's servers and stored on a web browser. Like most websites and search engines, Google uses cookies in order to provide a better user

EXCERPT FROM GOOGLE'S ADS AND ADVERTISING PRIVACY WEBPAGE

Read more information about interest-based advertising and the Ads Preferences Manager.

- **How to opt out of the DoubleClick cookie**

  You may choose to opt out of the DoubleClick cookie at any time.

  If you select the DoubleClick opt-out cookie, ads delivered to your browser by our ad-serving technology will not be served based on the DoubleClick cookie. Your DoubleClick opt-out cookie will not be uniquely identified. Other options on AdSense sites, partner sites and Google services that use the DoubleClick cookie may no longer be available; for example, we may no longer be able to prevent your browser from being served with the same ad over and over.

  As long as your browser retains the DoubleClick opt-out cookie, Google won't serve new DoubleClick cookies to your browser.

  Using a tool created by the Network Advertising Initiative, of which Google is a member, you can opt out of several third-party ad servers' and networks' cookies simultaneously.

- **Preserving your opt-out cookie**

  When you get a new computer, install a new browser, erase or otherwise alter your browser's cookie file (including upgrading certain browsers) you may also clear the cookies in your browser, including the DoubleClick opt-out cookie. Google offers a number of options to preserve your opt-out cookie.

Conversion Tracking Cookie

Google also uses a cookie to measure advertising performance for advertisers who have opted-in to conversion tracking on Google and its AdSense partners websites. The conversion tracking cookie is set when a user clicks on an ad delivered by Google where the advertiser has opted-in to tracking. These cookies expire within 30 days and are not personally-identifiable. If this cookie has not yet expired when the user visits certain pages of the advertiser's website, Google and the advertiser will be able to tell that the user clicked the ad and proceeded to that page. Each advertiser gets a different cookie, so no cookie can be tracked across advertiser websites.

- **How we use the conversion cookie information**

  We use the information collected by the conversion cookie to provide aggregate conversion stats to advertisers who have opted-in to conversion tracking. Advertisers are able to see the

James Comey, Director, Federal Bureau of Investigation

Brookings Institution, October 16, 2014

Good morning. It's an honor to be here.

I have been on the job as FBI Director for one year and one month. I like to express my tenure in terms of months, and I joke that I have eight years and 11 months to go, as if I'm incarcerated. But the truth is, I love this job, and I wake up every day excited to be part of the FBI.

Over the past year, I have confirmed what I long believed—that the FBI is filled with amazing people, doing an amazing array of things around the world, and doing them well. I have also confirmed what I have long known: that a commitment to the rule of law and civil liberties is at the core of the FBI. It is the organization's spine.

But we confront serious threats—threats that are changing every day. So I want to make sure I have every lawful tool available to keep you safe from those threats.

An Opportunity to Begin a National Conversation

I wanted to meet with you to talk in a serious way about the impact of emerging technology on public safety. And within that context, I think it's important to talk about the work we do in the FBI, and what we need to do the job you have entrusted us to do.

There are a lot of misconceptions in the public eye about what we in the government collect and the capabilities we have for collecting information.

My job is to explain and clarify where I can with regard to the work of the FBI. But at the same time, I want to get a better handle on your thoughts, because those of us in law enforcement can't do what we need to do without your trust and your support. We have no monopoly on wisdom.

My goal today isn't to tell people what to do. My goal is to urge our fellow citizens to participate in a conversation as a country about where we are, and where we want to be, with respect to the authority of law enforcement.

The Challenge of Going Dark

Technology has forever changed the world we live in. We're online, in one way or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. They hold much that is important to us.

And with that comes a desire to protect our privacy and our data—you want to share your lives with the people you choose. I sure do. But the FBI has a sworn duty to keep every American safe from crime and terrorism, and technology has become the tool of choice for some very dangerous people.

Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.

We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call "data in motion," such as phone calls, e-mail, and live chat sessions.

The second challenge concerns court-ordered access to data stored on our devices, such as e-mail, text messages, photos, and videos—or what we call "data at rest." And both real-time communication and stored data are increasingly encrypted.

Let's talk about court-ordered interception first, and then we'll talk about challenges posed by different means of encryption.

In the past, conducting electronic surveillance was more straightforward. We identified a target phone being used by a bad guy, with a single carrier. We obtained a court order for a wiretap, and, under the supervision of a judge, we collected the evidence we needed for prosecution.

Today, there are countless providers, countless networks, and countless means of communicating. We have laptops, smartphones, and tablets. We take them to work and to school, from the soccer field to Starbucks, over many networks, using any number of apps. And so do those conspiring to harm us. They use the same devices, the same networks, and the same apps to make plans, to target victims, and to cover up what they're doing. And that makes it tough for us to keep up.

If a suspected criminal is in his car, and he switches from cellular coverage to Wi-Fi, we may be out of luck. If he switches from one app to another, or from cellular voice service to a voice or messaging app, we may lose him. We may not have the capability to quickly switch lawful surveillance between devices, methods, and networks. The bad guys know this; they're taking advantage of it every day.

In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true. And unfortunately, the idea that the government has access to all communications at all times has extended—unfairly—to the investigations of law enforcement agencies that obtain individual warrants, approved by judges, to intercept the communications of suspected criminals.

Some believe that the FBI has these phenomenal capabilities to access any information at any time—that we can get what we want, when we want it, by flipping some sort of switch. It may be true in the movies or on TV. It is simply not the case in real life.

It frustrates me, because I want people to understand that law enforcement needs to be able to access communications and information to bring people to justice. We do so pursuant to the rule of law, with clear guidance and strict oversight. But even with lawful authority, we may not be able to access the evidence and the information we need.

Current law governing the interception of communications requires telecommunication carriers and broadband providers to build interception capabilities into their networks for court-ordered surveillance. But that law, the Communications Assistance for Law Enforcement Act, or CALEA, was enacted 20 years ago—a lifetime in the Internet age. And it doesn't cover new means of communication. Thousands of companies provide some form of communication service, and most are not required by statute to provide lawful intercept capabilities to law enforcement.

What this means is that an order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some can't comply, because they have not developed interception capabilities. Other providers want to provide assistance, but they have to build interception capabilities, and that takes time and money.

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren't seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology and to maintain our ability to actually collect the communications we are authorized to intercept.

And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks—all designed to increase security and privacy.

With Apple's new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple's announcement, Google announced plans to follow suit with its Android operating system. This means the companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within.

Both companies are run by good people, responding to what they perceive is a market demand. But the place they are leading us is one we shouldn't go to without careful thought and debate as a country.

At the outset, Apple says something that is reasonable—that it's not that big a deal. Apple argues, for example, that its users can back-up and store much of their data in "the cloud" and that the FBI can still access that data with lawful authority. But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement.

And if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what's on the phone who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data.

Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?

Correcting Misconceptions

Some argue that we will still have access to metadata, which includes telephone records and location information from telecommunications carriers. That is true. But metadata doesn't provide the content of any communication. It's incomplete information, and even this is difficult to access when time is of the essence. I wish we had time in our work, especially when lives are on the line. We usually don't.

There is a misconception that building a lawful intercept solution into a system requires a so-called "back door," one that foreign adversaries and hackers may try to exploit.

But that isn't true. We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process—front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.

Cyber adversaries will exploit any vulnerability they find. But it makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end—all in the name of privacy and network security.

Another misperception is that we can somehow guess the password or break into the phone with a so-called "brute force" attack. Even a supercomputer would have difficulty with today's high-level encryption, and some devices have a setting whereby the encryption key is erased if someone makes too many attempts to break the password, meaning no one can access that data.

Finally, a reasonable person might also ask, "Can't you just compel the owner of the phone to produce the password?" Likely, no. And even if we could compel them as a legal matter, if we had a child predator in custody, and he could choose to sit quietly through a 30-day contempt sentence for refusing to comply with a court order to produce his password, or he could risk a 30-year sentence for production and distribution of child pornography, which do you think he would choose?

Case Examples

Think about life without your smartphone, without Internet access, without texting or e-mail or the apps you use every day. I'm guessing most of you would feel rather lost and left behind. Kids call this FOMO, or "fear of missing out."

With Going Dark, those of us in law enforcement and public safety have a major fear of missing out—missing out on predators who exploit the most vulnerable among us...missing out on violent criminals who target our communities...missing out on a terrorist cell using social media to recruit, plan, and execute an attack.

Criminals and terrorists would like nothing more than for us to miss out. And the more we as a society rely on these devices, the more important they are to law enforcement and public safety officials. We have seen case after case—from homicides and car crashes to drug trafficking, domestic abuse, and child exploitation—where critical evidence came from smartphones, hard drives, and online communication.

Let's just talk about cases involving the content of phones.

In Louisiana, a known sex offender posed as a teenage girl to entice a 12-year-old boy to sneak out of his house to meet the supposed young girl. This predator, posing as a taxi driver, murdered the young boy and tried to alter and delete evidence on both his and the victim's cell phones to cover up his crime. Both phones were instrumental in showing that the suspect enticed this child into his taxi. He was sentenced to death in April of this year.

In Los Angeles, police investigated the death of a 2-year-old girl from blunt force trauma to her head. There were no witnesses. Text messages stored on her parents' cell phones to one another and to their family members proved the mother caused this young girl's death and that the father knew what was happening and failed to stop it. Text messages stored

on these devices also proved that the defendants failed to seek medical attention for hours while their daughter convulsed in her crib. They even went so far as to paint her tiny body with blue paint—to cover her bruises—before calling 911. Confronted with this evidence, both parents pled guilty.

In Kansas City, the DEA investigated a drug trafficking organization tied to heroin distribution, homicides, and robberies. The DEA obtained search warrants for several phones used by the group. Text messages found on the phones outlined the group's distribution chain and tied the group to a supply of lethal heroin that had caused 12 overdoses—and five deaths—including several high school students.

In Sacramento, a young couple and their four dogs were walking down the street at night when a car ran a red light and struck them—killing their four dogs, severing the young man's leg, and leaving the young woman in critical condition. The driver left the scene, and the young man died days later. Using "red light cameras" near the scene of the accident, the California Highway Patrol identified and arrested a suspect and seized his smartphone. GPS data on his phone placed the suspect at the scene of the accident and revealed that he had fled California shortly thereafter. He was convicted of second-degree murder and is serving a sentence of 25 years to life.

The evidence we find also helps exonerate innocent people. In Kansas, data from a cell phone was used to prove the innocence of several teens accused of rape. Without access to this phone, or the ability to recover a deleted video, several innocent young men could have been wrongly convicted.

These are cases in which we had access to the evidence we needed. But we're seeing more and more cases where we believe significant evidence is on that phone or a laptop, but we can't crack the password. If this becomes the norm, I would suggest to you that homicide cases could be stalled, suspects could walk free, and child exploitation might not be discovered or prosecuted. Justice may be denied, because of a locked phone or an encrypted hard drive.

My Thoughts

I'm deeply concerned about this, as both a law enforcement officer and a citizen. I understand some of this thinking in a post-Snowden world, but I believe it is mostly based on a failure to understand why we in law enforcement do what we do and how we do it.

I hope you know that I'm a huge believer in the rule of law. But I also believe that no one in this country should be above or beyond the law. There should be no law-free zone in this country. I like and believe very much that we need to follow the letter of the law to examine the contents of someone's closet or someone's cell phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.

I think it's time to ask: Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law? Are we so mistrustful of government—and of law enforcement—that we are willing to let bad guys walk away...willing to leave victims in search of justice?

There will come a day—and it comes every day in this business—where it will matter a great deal to innocent people that we in law enforcement can't access certain types of data or information, even with legal authorization. We have to have these discussions now.

I believe people should be skeptical of government power. I am. This country was founded by people who were worried about government power—who knew that you cannot trust people in power. So they divided government power among three branches, with checks and balances for each. And they wrote a Bill of Rights to ensure that the "papers and effects" of the people are secure from unreasonable searches.

But the way I see it, the means by which we conduct surveillance through telecommunication carriers and those Internet service providers who have developed lawful intercept solutions is an example of government operating in the way the founders intended—that is, the executive, the legislative, and the judicial branches proposing, enacting, executing, and overseeing legislation, pursuant to the rule of law.

Perhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction—in a direction of fear and mistrust. It is time to have open and honest debates about liberty and security.

Some have suggested there is a conflict between liberty and security. I disagree. At our best, we in law enforcement, national security, and public safety are looking for security that enhances liberty. When a city posts police officers at a dangerous playground, security has promoted liberty—the freedom to let a child play without fear.

The people of the FBI are sworn to protect both security and liberty. It isn't a question of conflict. We must care deeply about protecting liberty through due process of law, while also safeguarding the citizens we serve—in every investigation.

Where Do We Go from Here?

These are tough issues. And finding the space and time in our busy lives to understand these issues is hard. Intelligent people can and do disagree, and that's the beauty of American life—that smart people can come to the right answer.

I've never been someone who is a scaremonger. But I'm in a dangerous business. So I want to ensure that when we discuss limiting the court-authorized law enforcement tools we use to investigate suspected criminals that we understand what society gains and what we all stand to lose.

We in the FBI will continue to throw every lawful tool we have at this problem, but it's costly. It's inefficient. And it takes time.

We need to fix this problem. It is long past time.

We need assistance and cooperation from companies to comply with lawful court orders, so that criminals around the world cannot seek safe haven for lawless conduct. We need to find common ground. We care about the same things. I said it because I meant it. These companies are run by good people. And we know an adversarial posture won't take any of us very far down the road.

We understand the private sector's need to remain competitive in the global marketplace. And it isn't our intent to stifle innovation or undermine U.S. companies. But we have to find a way to help these companies understand what we need, why we need it, and how they can help, while still protecting privacy rights and providing network security and innovation. We need our private sector partners to take a step back, to pause, and to consider changing course.

We also need a regulatory or legislative fix to create a level playing field, so that all communication service providers are held to the same standard and so that those of us in law enforcement, national security, and public safety can continue to do the job you have entrusted us to do, in the way you would want us to.

Perhaps most importantly, we need to make sure the American public understands the work we do and the means by which we do it.

I really do believe we can get there, with a reasoned and practical approach. And we have to get there together. I don't have the perfect solution. But I think it's important to start the discussion. I'm happy to work with Congress, with our partners in the private sector, with my law enforcement and national security counterparts, and with the people we serve, to find the right answer—to find the balance we need.

Thank you for having me here today.