

FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

In The Matter Of)
Google Inc.'s Change)
In Data Use Policies)

Complaint, Request for Investigation, Injunction, and Other Relief

Submitted by

Consumer Watchdog

and

Privacy Rights Clearing House

Introduction

When Google acquired DoubleClick in 2007, it overcame significant privacy concerns by pledging to Congress, the Federal Trade Commission (FTC), and the public at large not to combine its users' personally-identifiable information with DoubleClick's vast browsing data.¹ These assurances paved the way for the FTC approval of the acquisition. Nearly a decade later, on June 28, 2016, Google quietly changed its privacy policy to permit the combination of this data, and forced the change on users in a highly deceptive manner, without meaningful notice and consent. The change marked the culmination of a nearly decade-long deception that Google has perpetrated against its users, the FTC, and the public at large. The change also violated legally binding commitments that Google made to the FTC.

Google took affirmative steps to conceal and downplay the significance of this transformational change that eliminated the barrier between the data that Google gathers from cookies that track users' behavior and the personal information that Google

¹ See Section I.B.1., *infra*; see also David Drummond, Senior Vice President of Corporate Development and Chief Legal Officer at Google, Statement to the Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights at 4 (Sept. 27, 2007) [hereinafter Drummond Statement], available at <https://www.judiciary.senate.gov/imo/media/doc/Drummond%20Testimony%2009272007.pdf>.

holds from its users' accounts. Google induced users to accept the change to its privacy policy by cloaking it in an offer to enable "new features" that purport to provide "more control" over users' personal information. Unsuspecting users accepted Google's offer in droves.

Google's June 2016 policy change marks a pivotal moment in Google's long-running shift on privacy. After meeting with widespread privacy concerns, Google had refrained for nearly a decade from combining its first-party consumer data with its third-party ad technology. In 2012, when Google significantly overhauled its privacy practices to enable it to combine a user's information across all Google properties, the company nonetheless maintained the separation between its users' account information and data on their browsing habits. When Google publicized its 2012 policy change, it drew heavy public criticism and congressional scrutiny.

Google apparently learned all of the wrong lessons from this experience. Despite the negative reaction to the incremental consolidation of its users' information, Google went forward with the 2016 change that finally dissolved the wall between consumer and browsing data. And rather than publicize this change, Google deceived its users as to its true nature and impact. With its latest change, Google finished demolishing the internal firewalls between its vast data-stores, eliminating the last vestige of Internet users' anonymity. This time, it did it with so little fanfare, and in so deceptive a manner that the media completely missed its true significance for nearly four months.²

Google has now created the "super-profiles" that privacy advocates warned against when Google acquired DoubleClick. But it has also gone significantly beyond what could have been envisioned at the time. Today, Google's trove of user data is orders of magnitude larger than it was when Google acquired DoubleClick. The company now has multiple properties with over 1 billion users each. When Google acquired DoubleClick, its policies required Google to keep a user's data segmented to a specific service—*e.g.*, data associated with a user's Gmail account would not be combined with data associated with his Maps account. Google's 2012 policy change, referenced above, eliminated this segmentation.

But the effects of the 2016 policy change did not stop there. The change enabled a whole new category of user tracking in ways that could scarcely have been contemplated in 2007. Google can now track users' activity on its Android mobile phones, with an 88% market share of smartphones worldwide,³ and from any website that uses Google Analytics, hosts YouTube videos, or displays ads served by DoubleClick or AdSense. In other words, Google has given itself the power to track users across the

² Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Information*, PROPUBLICA (Oct. 21, 2016) [hereinafter "Angwin Article"], available at <https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking>.

³ IDC, *Smartphone OS Market Share, 2016 Q2*, available at <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>.

overwhelming majority of websites in use in the world today, many of which appear to users to be entirely unconnected from Google.⁴

By finally combining all of this information, Google has engaged in a dangerously invasive and far-reaching appropriation of user data. And the manner in which Google perpetrated this appropriation makes it that much more vexing and legally actionable: Google has done incrementally and furtively what would plainly be illegal if done all at once.

The FTC has said that its enforcement actions “send an important message about the need to protect consumers’ privacy.”⁵ As this complaint will set out, Google is a serial reoffender. It has repeatedly violated consumers’ privacy and, when sanctioned, ignored its commitments to the FTC. Failing to take action now would send the message that as far as Google’s encroachments are concerned, consumers are on their own. Indeed, if the FTC fails to take action against the largest and most significant misappropriation of personal information—which is personal property—in the Internet era, other companies will be left to conclude that they too can avoid accountability. The public, for its part, would be left to question the value of the FTC and the ability of the Commission to protect consumers.

* * * * *

Google’s implementation of the June 2016 policy change is legally actionable for the following reasons:⁶

First, the policy change and the means by which it was implemented violate Section 5 of the FTC Act, which prohibits “unfair or deceptive acts or practices in or affecting commerce.”⁷ Google engaged in a string of deceptive acts, including: (i) representing that it would not combine its users’ personally-identifiable information with DoubleClick’s browsing data; (ii) repeatedly assuring its users that it would be transparent in how it handled their data; (iii) acquiring massive troves of its users’ data under false pretenses; and (iv) concealing the nature and extent of the change to its policies in order to obtain user consent. Each of these representations was intended to induce Google’s users to grant Google more and more access to their lives and their data.

⁴ Please see Appendix A for a discussion of the ad tech ecosystem, which provides background for understanding how Google monetizes personally-identifiable information through advertising.

⁵ Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission at 2, *In the Matter of Protecting the Privacy of Consumer of Broadband and Other Telecommunications Services*, FTC File No. 16-106 (May 27, 2016). The Commission vote authorizing staff to file the comment was 3-0. See <https://www.ftc.gov/news-events/press-releases/2016/05/ftc-staff-provides-comment-fccs-proposed-privacy-rulemaking>.

⁶ It is incumbent on the FTC to enforce Google’s violations. The FTC represents that it is “the leading U.S. consumer protection agency focused on commercial sector privacy,” and it is certainly the agency in this realm with the widest reach. While the Federal Communications Commission very recently adopted comprehensive privacy requirements on Broadband providers, these requirements do not reach “edge” companies like Google. That leaves the FTC with the sole responsibility for enforcing privacy protections provided by a number of companies that collect and profit from the unprecedented collection and exploitation of consumer data.

⁷ 15 U.S.C. § 45(a)(1).

Many users would likely not have granted this access if Google had been as transparent as it claimed. The Commission has taken action against companies who have engaged in similarly deceptive acts, including by filing a complaint against—and ultimately settling with—Facebook when the company broke promises to its users in connection with a 2009 policy change.⁸

Second, the policy change violated the terms of a Consent Order between Google and the FTC (Buzz Consent Order). Google is subject to a Consent Order because it misused its customers’ information during the rollout of the Google Buzz social network.⁹ Among other things, the Buzz Consent Order requires that Google not misrepresent the extent to which it (i) protects its users’ privacy and confidentiality; and (ii) adheres to the U.S.-EU Safe Harbor Framework. Google breached these obligations when it sought and obtained user consent to combine their personal information and browsing data by obscuring the nature and significance of this policy change.

* * * * *

For years, Google’s first line of defense against allegations of its monopoly power has been to argue that, on the Internet, “competition is only one click away.”¹⁰ As recent events have made troublingly clear, however, the “unique aspects of the Internet”¹¹ that Google has relied on as a defense likewise ensure that the privacy and security of U.S. citizens remain only one click away from dangerous hacks. As U.S. citizens are made increasingly vulnerable, the FTC’s role in protecting consumers from predatory data monopolies like Google becomes increasingly vital. Failing to protect the country’s consumers now would compromise the FTC’s core mission as envisioned by Louis Brandeis, and would further undermine the public’s confidence in the FTC as the last line of defense for our nation’s consumers.

I. Factual Background

A. June 2016 Policy Changes

1. Google’s Current Reach

Nearly a decade after its acquisition of DoubleClick and nearly five years since it began combining user data across its products, Google has obtained an unparalleled reach in the web-tracking and advertising realms and has continued to expand its suite of products and services, which are subsidized by user data. Google is

⁸ Press Release, *In the Matter of Facebook, Inc.*, FTC Docket No. C-4365 (2011), *available at* <http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceivedconsumers-failing-keep>.

⁹ See Section I.B.2., *infra*; see also Consent Order, *In re Google Inc.*, FTC File No. 102 3136, No. C-4336, at 4 (F.T.C. Oct. 24, 2011) [hereinafter Buzz Consent Order], *available at* <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf>

¹⁰ *E.g.*, *Google’s Approach to Competition*, Google Public Policy Blog (May 8, 2009), *available at* <https://publicpolicy.googleblog.com/2009/05/googles-approach-to-competition.html>.

¹¹ David Carr, *How Good (or Not Evil) Is Google?*, NEW YORK TIMES (June 21, 2009), *available at* http://www.nytimes.com/2009/06/22/business/media/22carr.html?pagewanted=2&_r=1&ref=technology.

now able to track users across the vast majority of Internet sites and mobile apps operating today. Those include a great number of sites and apps that most users would not suspect are in any way connected to the Internet giant.

A 2015 analysis of the tracking of web behavior found that “[a]lthough many companies track users online, the overall landscape is highly consolidated, with the top corporation, Google, tracking users on nearly 8 of 10 sites in the Alexa top 1 million.”¹² The company with the next highest figure, Facebook, was found on only 32.42% of sites.¹³ Google’s dominance in user tracking is paralleled by its dominance in the search advertising market. A leading source on digital advertising estimates that Google will generate \$57.8 billion in total digital ad revenue worldwide in 2016.¹⁴

As Google has expanded its advertising reach, it has also augmented its access to user information by expanding its user base. In 2015, Gmail surpassed a billion users, marking the seventh Google property to reach the milestone, joining Android, Chrome, Maps, Search, YouTube, and the Google Play Store.¹⁵ Google’s rise in the mobile market over the past decade has been particularly profound. Earlier this year, the European Commission (EC) sent a Statement of Objections to Google on Android, expressing its preliminary view that Google implemented a strategy on mobile devices to preserve and strengthen its dominance in general internet search.¹⁶

2. Implementation and Description of the Changes

On June 28, 2016, Google users were greeted with a notification headlined, “Some new features for your Google Account.” The notification continued:

We’ve introduced some optional features for your account, giving you more control over the data Google collects and how it’s used, while allowing Google to show you more relevant ads.¹⁷

The notification then asked the following question: “What changes if you turn on these new features?” The answer, according to the notification, was that “[m]ore information will be available in your *Google Account*, making it easier for you to review and control.” Even further down, the notification continued:

¹² Timothy Libert, *Exposing the Hidden Web: An Analysis of Third Party HTTP Requests on 1 Million Websites*, 9 INT’L J. OF COMMS. 3544 (2015). 1

¹³ *Id.* at 3553.

¹⁴ eMarketer, *Google Still Dominates the World Search Ad Market* (Jul. 26, 2016), available at <https://www.emarketer.com/Article/Google-Still-Dominates-World-Search-Ad-Market/1014258>

¹⁵ Xavier Harding, *Google Has 7 Products With 1 Billion Users*, POPULAR SCIENCE (Feb. 1, 2016), available at <http://www.popsoci.com/google-has-7-products-with-1-billion-users>.

¹⁶ European Commission, *Antitrust: Commission Sends Statement of Objections to Google on Android Operating System and Applications* (Apr. 20, 2016), available at http://europa.eu/rapid/press-release_IP-16-1492_en.htm.

¹⁷ See Appendix B for a copy of this notification.

When you use Google services like Search and YouTube, you generate data – things like what you’ve searched for and videos you’ve watched. You can find and control that data in *My Account* under the **Web & Apps Activity** setting.

With this change, this setting may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.

It was in this paragraph—which was included most of the way down the notification under a misleading headline stating that information in a user’s *Google Account* will be easier to control—that Google notified users that it had removed the barrier between the personal information that users share with Google and information gathered about those users from third-party sites and apps. This information includes not only user data from DoubleClick, but also data from third party apps on Android devices and all sites that use Google services, including, for example, browsing data from websites that use Google analytics, embed YouTube videos, and more. Google failed to inform users that it was combining one of the largest—if not the largest—corpus of consumer data with the world’s largest third party advertising platform. Google’s notification was a vast understatement, deceptively presented as a feature to enhance, not reduce, users’ privacy.

This change was reflected in a parallel amendment to Google’s Privacy Policy.¹⁸ Google struck out the language in the policy stating that it would “not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.” Now, Google told its users that it “may combine information from one service with information, including personal information, from other Google services,” and that users’ “activity on other sites and apps may be associated with your personal information in order to improve Google’s services and the ads delivered by Google.”

Users were not clearly informed of the significance of the changes—or “features” as Google would have it—nor were they clearly and unambiguously given a chance to reject them. Existing users who did not wish to accept the changes could not decline immediately, but instead were given the option to click “more options,” leading to a second notification. There, users could select “no changes,” which presumably meant that their personal data would not be combined with tracking data from third party sites and apps.

For new users, the combination of personal and browsing data was done by default. New users are notified that Google processes data from sources like Google Maps and from “apps or sites that use Google services like ads, Analytics, and the YouTube video player.”¹⁹ The notification later notes: “[w]e also combine data among our services and across your devices . . .”²⁰

¹⁸ See Appendix C.

¹⁹ See Appendix D.

²⁰ See Appendix E.

Anecdotally, many users who have activated the new features have no recollection of having done so, a testament to how deceptive the notice was. Google will almost certainly have extensively tested user responses to various versions of the notice, so the consumer reaction to its deceptive notice will likely have been very well understood by Google beforehand.

B. Google's Prior Relevant Conduct

Google's latest conduct is part of a pattern of behavior stretching back at least a decade. Since Google acquired DoubleClick in 2007, its policy standards have shifted—and have drawn public, regulatory and congressional scrutiny. In 2011, for example, Google entered into a Consent Order with the FTC to resolve allegations that it had deceived users about the treatment of their personal data in connection with the launch of its Google Buzz networking site.²¹ In 2012, Google paid \$22.5 million to settle FTC charges that the company violated the Buzz Consent Order by misrepresenting privacy assurances to users of Apple's Safari Internet browser.²² In those cases and others, Google has made a mockery of the "notice and consent" required by the FTC by systematically cloaking policy changes in deceptive language.

Google also implemented the policy overhaul, described above, that allowed them to combine the information users had provided with respect to various distinct Google products. In 2010, Google escaped significant penalties, despite admitting that it collected consumers' personal information through their WiFi networks without their knowledge, let alone permission. All of this conduct notwithstanding, Google has, from its acquisition of DoubleClick through to the present, continued to emphasize to users, regulators and Congress alike that transparency and user privacy are among the company's central tenets.

1. Google's Acquisition of DoubleClick

When it was acquired by Google, DoubleClick was already "the leading firm in the third party ad serving markets."²³ Third party ad servers help to manage the advertising space on websites, including by helping publishers identify advertisements that generate the greatest revenue.²⁴ In order to select which ads might generate the most revenue, DoubleClick "tracks" the activity of internet users. When a user is first shown, or "served" an ad, DoubleClick assigns the user a unique number and records that number in a "cookie" file stored on the user's computer. As that user visits other

²¹ Buzz Consent Order, *supra* note 9.

²² FTC, *Google Will Pay 22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (Aug. 9, 2012), available at <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>.

²³ Statement of the Federal Trade Commission at 6, *In the Matter of Google/DoubleClick*, F.T.C. File No. 071-0170 (Dec. 20, 2007) [FTC Google/DoubleClick Statement], available at

https://www.ftc.gov/system/files/documents/public_statements/418081/071220googlecdc-commstmt.pdf

²⁴ *Id.*

websites on which DoubleClick serves ads, he is identified as having viewed each ad.²⁵ Through these cookies, DoubleClick enabled advertisers to deliver ads to users based on pre-selected criteria, such as interest in sports, internet shopping habits, or algorithmically-determined age and gender.²⁶ DoubleClick maintained its tracking of user activity was anonymous—*i.e.*, that it could not be linked to an actual person through so-called personally-identifiable information.²⁷

Advocates warned, however, that the combination represented an unprecedented threat to Americans' privacy. The New York State Consumer Protection Board said, "[t]he combination of DoubleClick's Internet surfing history generated through consumers' pattern of clicking on specific advertisements, coupled with Google's database of consumers' past searches, will result in the creation of 'super-profiles,' which will make up the world's single largest repository of both personally and non-personally identifiable information."²⁸

In April 2007, Google reached an agreement to purchase DoubleClick for \$3.1 billion in cash, uniting the world's largest search advertising company with the largest digital display ad company. At the time of the acquisition, Google was already the dominant search engine in the US and in Europe.²⁹ Google also offered a number of non-search services, including Gmail, Google Maps, Google Talk, and YouTube.³⁰ Google generated most of its revenue from search and contextual ads³¹—*i.e.*, "ads that are delivered to a web page using technology that scans the text of a web page for key words and delivers ads to the page based on what the user is viewing."³² Google sold advertising to on third-party websites through its ad intermediation product, AdSense.³³

As part of the FTC's investigation of Google's potential acquisition, the Commission noted concerns "that the combination of [Google's and DoubleClick's] respective data sets of customer information could be exploited in a way that threatens consumers' privacy."³⁴ In particular, observers noted that Google had access to an unparalleled amount of information about its users, including data about its users' search queries and the ability to link those queries to Internet Protocol (IP) addresses they use.

²⁵ Complaint by the Electronic Privacy Information Center at 2, *In the Matter of Google/DoubleClick* (April 20, 2007) [hereinafter EPIC Google/DoubleClick Complaint], available at https://epic.org/privacy/ftc/google/epic_complaint.pdf.

²⁶ *Id.* at 3.

²⁷ In 1999, allegations emerged that DoubleClick was planning to combine its tracking data with detailed profiles from a national marketing database. After an investigation by the FTC, DoubleClick sold the data broker at a loss. Angwin Article, *supra* note 2.

²⁸ Marc Rotenberg, Executive Director Electronic Privacy Information Center, Statement to the Committee on Senate Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights, September 27, 2007, available at <https://www.gpo.gov/fdsys/pkg/CHRG-110shrg39015/pdf/CHRG-110shrg39015.pdf>.

²⁹ EPIC Google/DoubleClick Complaint, *supra* note 25, at 6.

³⁰ *Id.*

³¹ Louise Story and Miguel Helft, *Google Buys DoubleClick for \$3.1 Billion*, NEW YORK TIMES (Apr. 14, 2007), available at http://www.nytimes.com/2007/04/14/technology/14DoubleClick.html?_r=0.

³² FTC Google/DoubleClick Statement, *supra* note 23, at 5.

³³ *Id.* at 7.

³⁴ *Id.* at 2.

DoubleClick, on the other hand, tracked the browsing activities of Internet users, including by tracking consumers' pattern of clicking on specific advertisements.³⁵

Google vowed to protect users' data and to give them meaningful choices about how they would use it. In prepared remarks regarding the DoubleClick merger before the Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights, David Drummond, Google's then general counsel and now its Chief Legal Officer pledged: "privacy does not begin or end with our purchase of DoubleClick. Privacy is a user interest that we've been protecting since our inception."³⁶ He explained that Google spends "a lot of time designing products on the principles of transparency and choice - transparency about what information we collect and how we use it, and user choice about whether to provide us with personal information at all."³⁷

Drummond also made two concrete statements pertaining to the potential combination of the data collected by Google and DoubleClick. First, he explained that "DoubleClick is already extremely protective of privacy. In fact, it does not own and has very limited rights to use any of the data it processes on behalf of its publisher and advertiser clients."³⁸ In response to questioning from the committee, Drummond reiterated that DoubleClick's "data is owned by the customers – publishers and advertisers – and DoubleClick or Google can't do anything with it."³⁹ Second, Drummond said that Google was exploring using "crumbled" cookies. With crumbled cookies, user data would not be stored in association with a single cookie, such that it would not be clear that the data was coming from one person or machine.⁴⁰

Based on Google's representations, the FTC concluded that the transaction would not "adversely affect . . . consumer privacy."⁴¹ The Commission found that, as Drummond testified, "the customer and competitor information that DoubleClick collects currently belongs to publishers, not DoubleClick," and Google had "committed to the sanctity of those contracts."⁴² Commissioner Pamela Jones-Harbour dissented from the statement of reasons for closing the investigation out of concern that "the privacy interests of consumers" may not have been adequately addressed.⁴³ In what would turn

³⁵ Letter from Mindy Bockstein, Chairperson and Executive Director, New York State Consumer Protection Board, to Chairperson Deborah Platt Majoras, Federal Trade Commission (May 1, 2007).

³⁶ Drummond Statement, *supra* note 1, at 4.

³⁷ *Id.*

³⁸ *Id.*

³⁹ David Drummond, Senior Vice President of Corporate Development and Chief Legal Officer at Google, Testimony to the Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights, September 27, 2007, available at <https://www.gpo.gov/fdsys/pkg/CHRG-110shrg39015/pdf/CHRG-110shrg39015.pdf>.

⁴⁰ Drummond Statement, *supra* note 1, at 4.

⁴¹ FTC Google/DoubleClick Statement, *supra* note 23, at 2.

⁴² *Id.* at 11.

⁴³ Dissenting Statement of Commissioner Pamela Jones Harbour at 3, *In the Matter of Google/DoubleClick*, F.T.C. File No. 071-0170 (Dec. 20, 2007), available at <http://www.ftc.gov/os/caselist/0710170/071220harbour.pdf>.

out to be a prophetic statement, she expressed that she was “uncomfortable accepting the merging parties’ nonbinding representations at face value.”⁴⁴

The acquisition was a milestone for Google and it moved quickly to consolidate its grip on Internet advertising. Less than two years after the FTC approved Google’s acquisition of DoubleClick, Google acquired AdMob, “the world’s largest mobile advertising marketplace.” Advocacy groups—including Consumer Watchdog and the Center for Digital Democracy—expressed concern that combining the information Google had already amassed, including through its acquisition of DoubleClick, “would give Google a massive amount of consumer data to exploit for its benefit.”⁴⁵ Google responded to the letter by citing its “track record of providing strong privacy protections and tools . . . for users to take control or opt out of data collection,” and pledged to “apply the same approach to privacy following this acquisition.”⁴⁶

2. Google Buzz Launch and Consent Order

In 2010, Google launched a social networking site, Google Buzz (Buzz). The FTC charged that Google’s rollout of Buzz violated the FTC Act. When Buzz went live, Gmail users had to elect one of two options to proceed to their inboxes: “Sweet! Check out Buzz” or “Nah, go to my inbox.” The FTC found that users that selected to just proceed to their inboxes were nonetheless enrolled in certain of Buzz’s features. Even users who clicked “Sweet! Check out Buzz” were left uninformed of the implications of that selection. They were not informed, for example, that the identity of individuals they emailed most frequently would be made public by default. The FTC also found that Google deceived users as to the means by which they could unsubscribe from Buzz. While users were given the option to “turn off Buzz,” that option did not fully remove the user from the social network.⁴⁷

To settle the case and avoid any charges, in October 2011, Google entered into a binding Consent Order with the FTC. The order bars Google from misrepresenting the privacy or confidentiality of individuals’ information or misrepresenting compliance with the U.S.-EU Safe Harbor or other privacy, security, or compliance programs. The Order also requires that Google obtain affirmative opt-in consent before sharing users’ information with third parties if Google changes its products or services in a way that is contrary to any privacy promises made when the user’s information was collected.⁴⁸ Hinting at the growing skepticism of its promises, the FTC required Google to submit to monitoring of its promises for 20 years, an unusually long period.⁴⁹

⁴⁴ *Id.*

⁴⁵ Diane Bartz, *Advocacy Groups Urge FTC to Bar Google-AdMob Deal*, REUTERS (DEC. 28, 2009) [hereinafter AdMob Article], available at <http://www.reuters.com/article/us-google-admob-idUSTRE5BR2TA20091228>.

⁴⁶ *Id.*

⁴⁷ Complaint at 2-4, *In re Google Inc.*, FTC File No. 102 3136, at 4 (F.T.C. Oct. 24, 2011) [hereinafter Buzz Complaint], available at <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf>. *Id.* at 2-4.

⁴⁸ Buzz Consent Order, *supra* note 9, at 4.

⁴⁹ *Id.*

Google framed the launch of Buzz as nothing more than an uncharacteristic lapse in its commitment to transparency and consumer privacy, stating: “We try very hard to be upfront about the data we collect, and how we use it, as well as to build meaningful controls into our products . . . [o]f course we do not get everything 100 percent right.”⁵⁰

3. Policy Change: Combining Data Across Google Services

Less than four months after entering into the Buzz Consent Order, Google announced plans to fundamentally change its privacy policy and terms of service.⁵¹ The most significant change was that, while Google had previously kept users’ data from each of its services separate, it was now fusing all of that data together.

Influenced by the recent Consent Order, Google announced the change two months before it took effect in a blog post that stated clearly: **The main change is for users with Google Accounts. Our new Privacy Policy makes clear that, if you’re signed in, we may combine information that you’ve provided from one service with information from other services.**⁵² The post also contained a video that was intended to provide a simple explanation of the shift. Google undertook extensive efforts to obtain public support for the policy change. The company posted advertisements everywhere from the New York City subways to the World Wide Web. The advertisements offered simplified explanations of things like “cookies,” and declared “[w]e’re changing our Privacy Policy. Not your privacy controls.”⁵³ Google emphasized that it remained committed to being “transparent about the information [Google] collects.”⁵⁴ Clearly, Google was proactively taking steps to head off any claim that it did not adequately inform users.

Google was criticized because it did not give users the ability to opt out of the change. The FTC declined to take action. A number of global authorities, however, found that Google’s new policies were in conflict with their countries’ data protection laws. In October 2012, the Article 29 Working Party—a group comprised of representatives of national data protection authorities from EU member states—issued the results of its investigation into Google’s new privacy policy, concluding that Google had breached European data protection law on multiple grounds.⁵⁵

⁵⁰ Declan McCullagh, *Privacy Officials Criticize Launch of Google Buzz*, CNET (Apr. 21, 2010), available at <https://www.cnet.com/au/news/privacy-officials-criticize-launch-of-google-buzz/>.

⁵¹ *Updating Our Privacy Policies and Terms of Use*, Google Official Blog (Jan. 24, 2012), available at <https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html>.

⁵² *Id.* (emphasis added).

⁵³ Adi Robertson, *Google Strikes Back Against Privacy Policy Fears with New Ads*, THE VERGE (Feb. 1, 2012), available at <http://www.theverge.com/2012/2/1/2764033/google-privacy-policy-change-ads>.

⁵⁴ Letter from Pablo Chavez, Director of Public Policy, Google Inc., to Hon. Sen. Cliff Stearns, et al at 2 (Jan. 30, 2012) [hereinafter Chavez Letter], available at <http://its.ucsc.edu/email/docs/google-letter-about-privacy.pdf>.

⁵⁵ Initiative for a Competitive Online Marketplace, *The Google Privacy Investigation in Europe: Two Years On* at 1 (Oct. 2014), available at <http://i-comp.org/wp-content/uploads/2014/10/The-Google-Privacy-Investigation-in-Europe-Two-Years-On4.pdf>.

4. Tracking of Safari Users

In February 2012, just as Google was preparing to consolidate user information across all Google Services, a Stanford researcher discovered that Google was bypassing the privacy settings of Apple's Safari Web-browser in order to surreptitiously and deceptively track web users' online activities.⁵⁶

Google had offered users wary of having their online activities tracked the option to "opt out" of targeted advertising. One way to opt-out was to install an "opt-out cookie" plugin. The plugin was not technologically available for Safari and Google represented that such a plugin would in any event be unnecessary, because the Safari default setting "effectively accomplishes the same thing as setting the opt-out cookie."⁵⁷ The FTC alleged that Google used an invisible code to circumvent Safari's protections and set cookies, including DoubleClick advertising cookies, in the user's browser.

The FTC charged that Google's conduct violated the Buzz Consent Order. The parties reached an agreement in August 2012, under which Google was required to pay a \$22.5 million fine and undertake remedial action.⁵⁸ Google once again held that it was an uncharacteristic lapse. Following the settlement Google declared, "[w]e set the highest standards of privacy and security for our users," and argued that the FTC's investigation was "focused on a 2009 help center page," rather than taking responsibility for violating the privacy of millions of users.⁵⁹

5. "Wi-Spy"

In 2010, it was revealed that as part of Google's project to populate its "Street View" feature, which provides images from positions along a number of streets, Google "collected data from Wi-Fi networks throughout the United States and around the world."⁶⁰ The data Google collected included "payload" data—*i.e.*, the content of Internet communications, including e-mails, text messages, passwords, Internet usage history, and other highly sensitive personal information.⁶¹

⁵⁶ Julia Angwin and Jennifer Valentin-Devries, *Google's iPhone Tracking*, WALL STREET JOURNAL (Feb. 17, 2012), available at <http://www.wsj.com/articles/SB10001424052970204880404577225380456599176>.

⁵⁷ Complaint for Civil Penalties and Other Relief at 7, *United States v. Google, Inc.*, No. CV 12-04177 HRL (N.D. Cal. Aug. 8, 2012), available at

<https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf>

⁵⁸ Stipulated Order for Permanent Injunction and Civil Penalty Judgment, *United States v. Google, Inc.*, No. CV 12-04177 HRL (N.D. Cal. Aug. 8, 2012), available at

<https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlestip.pdf>.

⁵⁹ Katy Bachman, *Google to Pay Record \$22.5 Million to Settle with FTC*, ADWEEK, (Aug. 9, 2012), available at <http://www.adweek.com/news/technology/google-pay-record-225-million-settle-ftc-142646>

⁶⁰ Notice of Apparent Liability for Forfeiture, *In the Matter of Google Inc.*, FCC File No. EB-10-IH-4055 (Apr. 13, 2013) [hereinafter FCC Wi-Spy Notice].

⁶¹ *Id.*

Google initially denied claims that it had collected payload data.⁶² When it eventually acknowledged publicly that it had collected that data, “Google said it was an accident, due to code mistakenly created by a rogue engineer.”⁶³

A number of agencies investigated Google’s conduct, including the FCC, the FTC, and state attorneys general. The FCC found that “[f]or many months, Google deliberately impeded and delayed the Bureau’s investigations by failing to respond to requests for material information and to provide certifications and verifications of its responses.”⁶⁴ The FCC found Google liable for a \$25,000 penalty for its noncompliance, but found “no clear precedent” for applying the Communications Act to Google’s underlying conduct.⁶⁵ The FTC ended its inquiry based on certain “commitments” Google made—including “adding core privacy training for key employees” and promising not to “use any of the payload data collected in any Google product or service.”⁶⁶ Google entered into a \$7 million multistate settlement with 38 state attorneys general to resolve their investigation.⁶⁷

II. Argument

When Google launched Buzz in 2010, it implemented a byzantine opt-out process that left many unaware that they were still enrolled in the service. The FTC found this practice misleading, and ultimately entered into a binding Consent Order with Google, which required Google to be more transparent in the manner in which it handles customer data. Yet in launching its revised June 2016 policy, Google once again employed a confusing, multi-step process that left users clueless as to the nature of the changes and misled as to how to avoid them.

Likewise, in 2012—while Google was subject to the Buzz Consent Order—it was revealed that the company had been misleading Safari browser users about the extent to which it was tracking their activity. Google was punished for this indiscretion with a fine. Now again, in introducing its June 2016 policy change, Google has used a deceptive notification to conceal from users the scope of the data that Google can collect and combine.

It is clear that Google is operating without fear that it could be held to account for its conduct. Google is a serial offender, and the action that the FTC has taken to date has done nothing to slow Google’s intrusive violations of its users’ privacy. The

⁶² *Id.*

⁶³ Kashmir Hill, *Wi-Spy Google Engineer Outed as ‘Hacker’ God’ Marius Milner*, FORBES (May 1, 2012), available at <http://www.forbes.com/sites/kashmirhill/2012/05/01/wi-spy-google-engineer-outed-as-hacker-god-marius-milner/#2a3524a8327e>

⁶⁴ FCC Wi-Spy Notice, *supra* note 60, at 2.

⁶⁵ *Id.*

⁶⁶ Letter from David C. Vladeck, Director FTC’s Bureau of Consumer Protection, to Albert Gidari (Oct. 27, 2010), available at https://www.ftc.gov/sites/default/files/documents/closing_letters/google-inquiry/101027googleletter.pdf.

⁶⁷ Attorney General George Jepson, *Attorney General Announced \$7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data* (Mar. 12, 2013), available at <http://www.ct.gov/ag/cwp/view.asp?Q=520518>.

FTC must act now, and act with enough force to dissuade Google from further destructive behavior. If the Commission does not impose a significant punishment on Google for its repeat offenses, it must relinquish its mandate to enforce privacy protections to a competent agency that can protect consumers' privacy.

The FTC has clear legal grounds for taking action. Google's conduct since its acquisition of DoubleClick—culminating in the implementation of its June 2016 policy change—violated both Section 5 of the FTC Act and the requirements of Buzz Consent Order. The latest change is part of a pattern of deception that has gone unpunished and undeterred for too long.

FTC Section 5

Section 5 prohibits “unfair or deceptive acts or practices in or affecting commerce.”⁶⁸ A deceptive trade practice is defined as a “misrepresentation, omission or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment.”⁶⁹ This definition can be broken down into three requirements: (1) an act (representation, omission, or practice), (2) the likelihood of a reasonable consumer's deception, and (3) materiality.

1. Google Has Made a Series of False and Misleading Representations

The FTC has long stressed the importance of “giving consumers information and choices about their data,”⁷⁰ and it has found representations like those made by Google to be misleading. In a complaint that the FTC filed against Snapchat, for example, the Commission noted that “Snapchat marketed its application as a service for sending ‘disappearing’ photo and video messages.”⁷¹ In contrast to these marketing statements and other similar representations, however, the Commission found that “several methods exist by which a recipient can use tools outside of the application to save both photo and video messages.”⁷²

Just as Snapchat emphasized the ephemeral nature of its messages in its marketing, Google made explicit representations (i) that it could not “do anything with” the browsing data that it would acquire through the acquisition of DoubleClick; and (ii) that it would be “transparent about the information [it] collects” and would provide “meaningful choices about how it is used.” Indeed, Google's misrepresentations—some of which were made under oath before a Congressional committee—were far more significant than were Snapchat's marketing statements. These representations were proven false when, in June 2016, Google quietly took down the wall between the data

⁶⁸ 15 U.S.C. § 45(a)(1).

⁶⁹ Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983) [hereinafter Deceptiveness Statement].

⁷⁰ Fed. Trade Comm'n, *Internet of Things* at vii (Nov. 2013), available at <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

⁷¹ Complaint at 2, Snapchat, Inc., Docket No. C-4501 (May 8, 2014).

⁷² *Id.*

that it gathers from the cookies that track web browsing behavior and the personal information that Google holds from its users' accounts.

The FTC has also characterized as misleading efforts to obtain user consent to policy changes without sufficiently notifying users as to the extent of those changes. The Commission charged Facebook with misleading customers based on its December 2009 rollout of a policy change. To implement the change, "Facebook required each user to click through a multi-page notice, called the Privacy Wizard."⁷³ The Wizard required users to "choose between new privacy settings . . . and the user's old settings."⁷⁴ The Commission found Facebook's notification to users to be misleading because the Wizard "did not disclose adequately that users no longer could restrict access to their newly-designated" publicly-available information and that this information would be accessible to the public.⁷⁵

Here, Google required existing users to click through a notification announcing their accounts' "new features," which ostensibly gave the users "more control over the data Google collects and how it's used." The notification referenced the combination of the two data tranches two-thirds of the way down the page and in an oblique manner, telling users that their "Web & App Activity setting" might include "activity from sites and apps that partner with Google." This notification (and the accompanying change to Google's privacy policy) was misleading as it did not adequately disclose the nature, intent or extent of Google's policy change.

2. A Reasonable User Would be Deceived By Google's Conduct

According to FTC guidance, "an interpretation will be presumed reasonable if it is the one the respondent intended to convey."⁷⁶ It is clear that Google intended to convey to users, agencies, and the public that (i) it would not combine user and browsing data; and (ii) that its June 2016 policy changes were minor and would benefit its users, thereby concealing that the revised policy actually marked a sea change that would have a sweeping a deleterious effect on their privacy, making it virtually impossible to escape Google's tracking of them. Google's misrepresentations allowed it to obtain the dominant market positions it has amassed—market positions that render the company's 2016 change in policy such a serious threat to American consumers.

Even before Google acquired DoubleClick, consumers and the FTC expressed concerns that DoubleClick could connect the troves of browsing data that it had access to with personal information of people who use the Web.⁷⁷ These concerns were elevated when Google—with its extensive libraries of user information and search histories—sought to acquire DoubleClick. Google assuaged fears that it might create "superprofiles" of its users by swearing before Congress that the contract structures that DoubleClick had in place—which Google vowed to honor—would prevent Google from

⁷³ Complaint at 7-9, *In re Facebook, Inc.*, FTC File No. 092 3184, No. C-4365 (F.T.C. July 27, 2012).

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ Deceptiveness Statement, *supra* note 72, at 3.

⁷⁷ FTC Google/DoubleClick Statement, *supra* note 23, at 5.

doing “anything” with the DoubleClick data. Google also swore that its products were built on the “principles of transparency and choice,” that the company would be open about the user information it collected, and that it would allow users the opportunity to decide whether to grant Google access to their information at all.⁷⁸ The public and agencies like the FTC relied on these representations, both when approving the DoubleClick acquisition and when evaluating Google’s subsequent course of conduct. Google’s users were willing to grant Google more access to their personal information and governmental agencies were willing to allow Google to expand its reach in ways that they never would have had Google not made these ultimately false assurances.

Less than two years after approving Google’s acquisition of DoubleClick, the FTC permitted Google to further widen its reach through its purchase of AdMob, “the world’s largest mobile advertising marketplace.” Google pledged to apply the “the same approach to privacy” that had earned it approval of the DoubleClick acquisition.⁷⁹ In 2010, when Google misused its customers’ data in launching Buzz, it made assurances that this was an uncharacteristic mistake and that Google remained a company committed to being “upfront” with its users about its handling of their data.⁸⁰

In 2012, Google changed its policies to permit the company to combine its users’ data across all Google products. This was a significant change from Google’s prior practice, and one that was a precursor to and necessary incremental step towards the June 28, 2016 policy change. Google cited to the manner in which it announced the 2012 policy change as a “great example” of the Company’s “effort to lead the industry in transparency.”⁸¹ In hindsight, however, the announcement was another in a string of Google’s highly deceptive actions. Google was only able to obtain public and governmental approval for the policy change because the public and governmental agencies understood, based on Google’s prior representations, that even if Google’s user data were consolidated across Google products, that consolidated data could not be combined with the web browsing data that Google tracked via DoubleClick and other services.

In sum, the position that Google was in on June 27, 2016—a company with multiple billion-user products and a dominant or leading position over every link in the ad tech supply chain—was made possible because Google deceived the public and governmental agencies alike that it was sensitive to concerns regarding its handling of user data, that it would ensure that its policies reflected that sensitivity, and, most of all, that it would maintain its policy that prohibited Google from combining DoubleClick cookie information with personally identifiable information absent explicit and informed opt-in consent.

The manner in which Google attempted to convince its users to agree to its monumental June 28, 2016 policy shift—a shift that exploited the consumer and governmental reliance it had built over the prior decade—further underscores the fact and

⁷⁸ See Section I.B.1., *supra*.

⁷⁹ AdMob Article, *supra* note 45.

⁸⁰ See Section I.B.2., *supra*.

⁸¹ Chavez Letter, *supra* note 54, at 2.

extent of Google’s deception. The notification that greeted existing users barely hinted at the policy change, vaguely informing them that their accounts now “may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.”⁸²

This announcement intentionally misled users, who had no way to discern from the wording that Google was breaking from a nearly decade-old practice and asking them if it could link their personal information to data reflecting their behavior on as many as 80% of the Internet’s leading websites. A reasonable user would have been left with precisely the impression Google was seeking to leave: that the 2016 change was to their benefit and posed no risk to their privacy. In reality, the policy change marked the consummation of a deceptive path that Google had methodically charted since it first sought to acquire DoubleClick in 2007.

3. Google’s Misrepresentations were Material

With respect to materiality, the basic question is “whether the act or practice is likely to affect the consumer’s conduct or decision with regard to a product or service.” Google misrepresented the manner in which it would handle its users’ data precisely because it knew that users’ privacy concerns would dictate the extent to which they would be willing to entrust their data to Google. If Google had not deceived its users regarding its handling of their data, it is possible that many users would not have entrusted their data to Google to begin with, let alone allowed Google to combine all of that data for use in invasive and all-encompassing targeted advertising.

The context data that Google has access to and has now combined is increasingly exploited by companies in the online advertising sphere. The June 2016 policy change permits Google to grab data from any website that uses Google Analytics, hosts YouTube videos, displays ads served by DoubleClick or AdSense—the overwhelming majority of sites in use in the world today—combine that information with user account data, and then deploy that information to target advertisements over the entire internet and app ecosystem. Google appears to already be putting these invasive new capabilities into action.

In September, ahead of New York Advertising Week, Google introduced several new advertising “innovations” on its AdWords blog.⁸³ Two of these innovations seemed to have been made possible by the June 2016 policy change. The first “innovation” was touted as allowing advertisers to “close the loop” by tracking and targeting individual customers across all of their electronic devices: say, their desktop at work, the phone on the subway and a tablet at home. Previously, cookies (on computers) and Advertising IDs (on mobile devices) tracked user activity and built profiles for browsing behavior on each device, but these data stores were kept apart.⁸⁴ While

⁸² See Section I.A.2.

⁸³ *New Digital Innovations to Close the Loop for Advertisers*, Google Inside AdWords (Sept. 25, 2016), available at <https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html>

⁸⁴ *Id.*

Google's old privacy policy effectively forbade this consolidated profiling, the June 2016 policy permits the unification of activity data across all of a user's devices. The second "innovation" contemplates combining a user's location with data from their accounts.⁸⁵ The company provides a glimpse into how advertisers might use this new, richer data on its market research microsite, "Think with Google." The site coaches advertisers on how to reach customers at their most impressionable 'micro-moments,' such as searching for a cold-sore medication in the drugstore, dealing with a medical crisis, or struggling to use equipment for a new baby.⁸⁶ "Only Google has the scale and the tools to help you reach people in the moments that truly matter and measure impact across devices and channels," Google said in its post.⁸⁷

This level of invasion would clearly be material to users' prior decisions to grant Google access to many aspects of their lives and to their more recent decision as to whether to consent to Google's policy change.

B. Buzz Consent Order

Google also violated Section I of the Buzz Consent Order through the misrepresentations described above and by failing to clearly disclose the changes to its privacy policy before obtaining consent from users to change the way in which it handled those users' data.

1. Section 1(a) of the Buzz Consent Order

Section 1(a) of the Buzz Consent Order establishes that Google cannot:

[M]isrepresent in any manner, expressly or by implication 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.⁸⁸

As described in Section II.B.1., *supra*, Google has, since its acquisition of DoubleClick, misled its users as to its maintenance and protection of their information by representing that their personal and web browsing data would not be combined and by representing that it would be transparent in the manner in which it handled customer data. These misrepresentations allowed Google to amass significant amounts of data about its users. Google then misled users as to the extent to which they could exercise control over

⁸⁵ Google AdWords, *Bridging the Customer Journey Across the Physical and Digital Worlds* [hereinafter *Bridging the Customer Journey*], available at <https://static.googleusercontent.com/media/www.google.com/en/us/adwords/start/marketing-goals/pdf/white-paper-bridging-the-customer-journey.pdf>.

⁸⁶ Think with Google, *Micro-Moments*, available at <https://www.thinkwithgoogle.com/micromoments/intro.html>.

⁸⁷ *Bridging the Customer Journey*, *supra* note 88.

⁸⁸ Buzz Consent Order, *supra* note 9, at 3-4.

the collection, use, or disclosure this covered information by obtaining their consent to combine their personal and web browsing data through deceptive means.

2. Section 1(b) of the Buzz Consent Order

Section I(b) of the Buzz Consent Order establishes that Google cannot:

[M]isrepresent in any manner, expressly or by implication 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.⁸⁹

The U.S.-EU Safe Harbor Framework provided a method for U.S. companies to transfer personal data outside the EU that was consistent with the requirements of the European Union Data Protection Directive. U.S. companies could voluntarily enroll in Safe Harbor by self-certifying that they complied with seven principles and related requirements that were deemed to meet the EU's adequacy standards.⁹⁰ From October 2005 until October 2016, Google maintained a self-certification and appeared on the list of Safe Harbor companies on the Commerce website.⁹¹ Pursuant to the Safe Harbor Frequently Asked Questions on Self-Certification, the commitment to adhere to the Safe Harbor Principles is not time-limited, and a participating organization must continue to apply the Principles to data received under the Safe Harbor.⁹² In August 2016, the Safe Harbor Framework was replaced by the EU-U.S. Privacy Shield Program. Google is an active member of the Privacy Shield Framework.⁹³

Both the Safe Harbor and Privacy Shield Frameworks require that organizations notify individuals about the purposes for which they collect and use information about them.⁹⁴ Both Frameworks likewise require that “[a]n organization must offer individuals the opportunity to choose (opt out) whether their personal information is . . . to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual.

⁸⁹ *Id.*

⁹⁰ In October 2015, the European Court of Justice issued a judgment declaring as “invalid” the European Commission’s prior decision that the Safe Harbor provides adequate protections. Safe Harbor has been replaced with a Framework called Privacy Shield. As of October 31, 2016, the Department of Commerce will stop accepting Safe Harbor applications.

⁹¹ Export.gov, *U.S.-EU Safe Harbor List*, available at <https://safeharbor.export.gov/list.aspx>

⁹² *Id.*

⁹³ *Id.*

⁹⁴ U.S. Dep’t of Commerce, *U.S.-EU Safe Harbor Framework Guide to Self-Certification* at 3 (2009), available at <http://www.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf>; U.S. Dep’t of Commerce, *EU-U.S. Privacy Shield Framework Principles* at 4 (2016), available at <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>

Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.”⁹⁵

By combining users’ personal and web browsing data, Google was using its users’ personal information for a purpose that was incompatible with the purpose for which it was originally collected. Under the EU Frameworks, Google was thus required to obtain its users’ consent before combining the two data tranches. The notice that Google provided was deficient. It was buried on a page touting the users’ increased control over their information, and merely told users that their “Web & Apps Activity” setting “may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.” An ordinary consumer would not comprehend from the placement and content of this notification that Google had departed from its prior policy of keeping separate users’ personal information and web browsing behavior.

Based on the foregoing, FTC must take swift action to protect consumers and hold Google accountable for its sweeping and deceptive June 2016 policy change.

III. Prayer for Investigation and Relief

Petitioners request that the Commission investigate and enjoin Google from engaging in unfair business practices in connection with its data collection policies and practices. Specifically, petitioners request that the Commission:

- Investigate Google’s data gathering polices and changes thereto announced in June 2016;
- Investigate the adequacy of Google’s notice to users of changes in its data and privacy policies;
- Investigate whether Google’s data collection policies and practices violate the Buzz Consent Agreement;
- Enjoin Google from combining data gathered from its Doubleclick subsidiary with data gathered from its other services without meaningful informed user consent;
- Order Google to sever data gathered from its Doubleclick subsidiary that has been combined with data gathered from its other services since June 2016;
- If the Commission finds that Google’s data collection policies and practices violate the Buzz Consent Agreement, fine Google appropriately for its second violation of the Buzz Consent Agreement;

⁹⁵ *Id.*

- Order Google to disgorge and return advertising revenues obtained as a result of combining data gathered from its Doubleclick subsidiary with data gathered from its other services after an unfair and deceptive notice to users of such practice in June 2016; and
- Provide other such relief as the Commission finds necessary and appropriate.

Respectfully Submitted,

John M. Simpson, Privacy Project Director

CONSUMER WATCHDOG
1750 Ocean Park Blvd., Suite 200
Santa Monica, CA 90405
Phone: (310) 392-0522
Fax: (310) 392-8874
www.ConsumerWatchdog.org

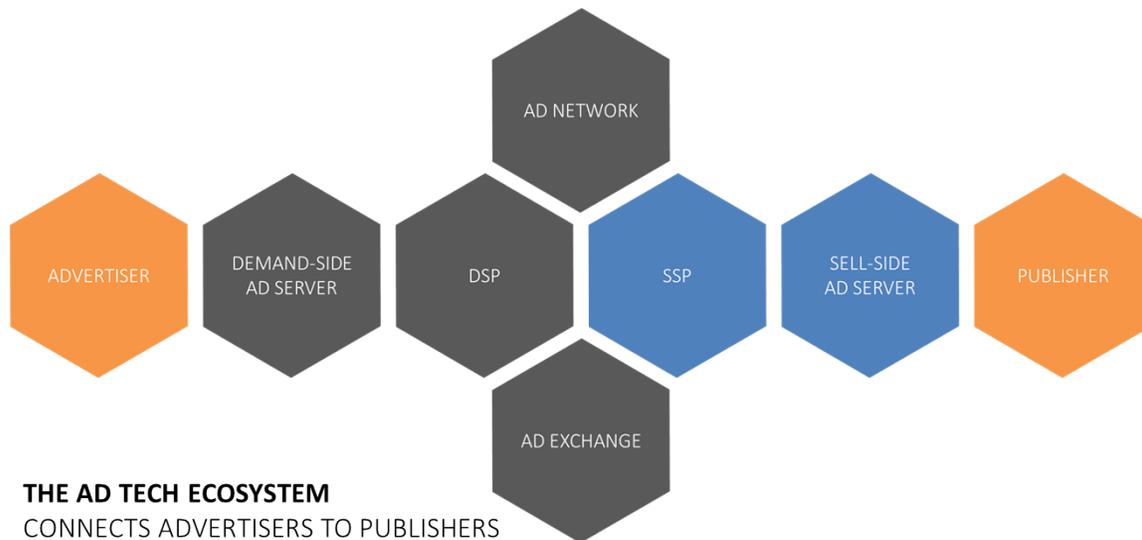
Beth Givens, Founder and Executive
Director

PRIVACY RIGHTS CLEARINGHOUSE
3033 Fifth Ave., Suite 223
San Diego, CA 92103
619) 298-3396
www.privacyrights.org

Appendix A

In order to understand how Google now monetizes personally-identifiable information through advertising, it is important to have a basic understanding of the ad tech ecosystem that makes online advertising possible. Before an ad can appear it must first pass through a variety of ad tech tools. These ad tech tools interconnect with one another, forming a supply chain linking publishers and developers on one side to advertisers on the other.

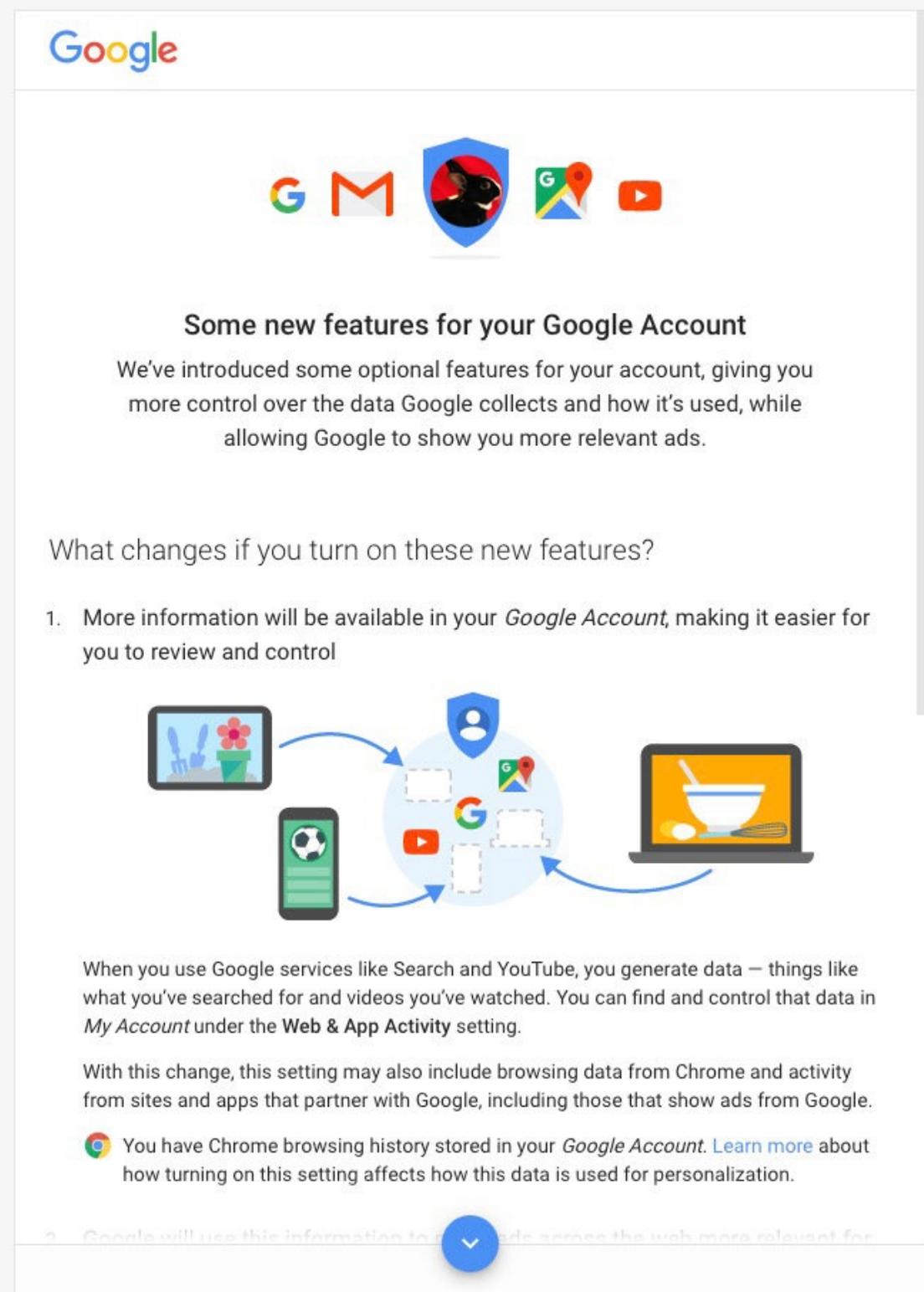
Different ad tech tools serve different functions. For example, “ad networks” aggregate advertising space—“inventory”—from many different publishers and developers, creating a centralized location for advertisers to shop. “Ad exchanges” serve as online marketplaces, enabling advertisers to programmatically bid in real time on inventory-meeting-specified characteristics. “Demand-side platforms” (“DSPs”) and “supply-side platforms” (“SSPs”) help advertisers and publishers/developers respectively to broaden their reach, enabling them to find and execute transactions that might not otherwise take place. Finally, “ad servers” perform the actual task of displaying an ad on a website or app, keeping track of how the user interacts with the ad, and managing yield among various advertising channels.



Beginning with its acquisition of DoubleClick (*see supra*), Google has amassed a dominant position over every link in the ad tech supply chain. Google presently controls the largest ad networks (Google Display Network, AdSense, and AdMob), ad exchange (DoubleClick Ad Exchange), DSP (DoubleClick Bid Manager), SSP (AdMeld, now part of DoubleClick Ad Exchange), and ad servers (DoubleClick for Publishers and DoubleClick Campaign Manager). Google’s omnipresence in the ad tech pipeline means that the vast majority of display ads bought and sold online pass at some point through a Google-owned ad tech property. The vast majority of online and mobile ads passes through at one of Google/DoubleClick’s dominant ad tech properties, each of which benefit from personal user data.

Appendix B

Top of Google's deceptive notice to users about the June 28, 2016 privacy policy change:



The image is a screenshot of a notification banner from Google. At the top left is the Google logo. In the center, there are five icons: the 'G' and 'M' from Gmail, a shield with a black silhouette of a person's head, the 'G' and a location pin from Google Maps, and the YouTube play button. Below these icons is the heading "Some new features for your Google Account". The main text reads: "We've introduced some optional features for your account, giving you more control over the data Google collects and how it's used, while allowing Google to show you more relevant ads." Below this is the question "What changes if you turn on these new features?" followed by a numbered list item: "1. More information will be available in your *Google Account*, making it easier for you to review and control". Underneath the list item is a diagram showing a central blue circle with a shield icon and the Google 'G' logo. Four arrows point from this central circle to four different devices: a tablet showing a garden scene, a smartphone showing a soccer ball, a laptop showing a bowl of soup, and another tablet showing a person's profile. Below the diagram is the text: "When you use Google services like Search and YouTube, you generate data — things like what you've searched for and videos you've watched. You can find and control that data in *My Account* under the **Web & App Activity** setting." This is followed by another paragraph: "With this change, this setting may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google." Below that is a bullet point with the Chrome logo: "You have Chrome browsing history stored in your *Google Account*. [Learn more](#) about how turning on this setting affects how this data is used for personalization." At the bottom of the banner, there is a blue circular button with a white downward-pointing chevron. Below the button, the start of a second list item is visible: "2. Google will use this information to r... ads across the web more relevant for".

Google

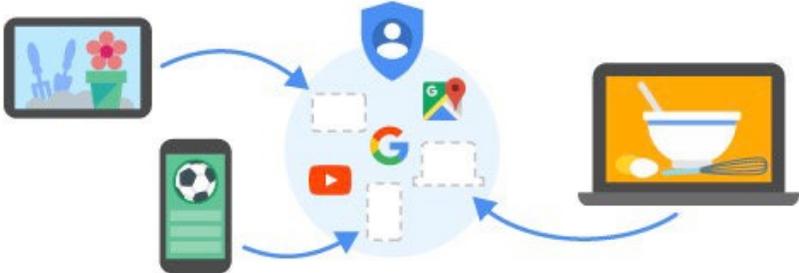
G M [Shield icon] [Maps icon] [YouTube icon]

Some new features for your Google Account

We've introduced some optional features for your account, giving you more control over the data Google collects and how it's used, while allowing Google to show you more relevant ads.

What changes if you turn on these new features?

1. More information will be available in your *Google Account*, making it easier for you to review and control



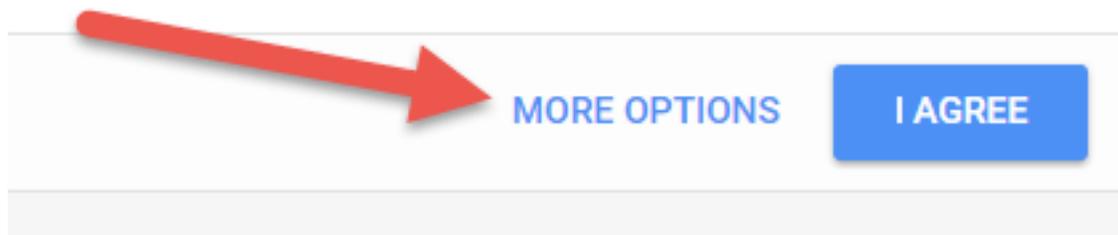
When you use Google services like Search and YouTube, you generate data — things like what you've searched for and videos you've watched. You can find and control that data in *My Account* under the **Web & App Activity** setting.

With this change, this setting may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.

- You have Chrome browsing history stored in your *Google Account*. [Learn more](#) about how turning on this setting affects how this data is used for personalization.

2. Google will use this information to r... ads across the web more relevant for

Bottom of Google's notice to users about the June 28, 2016 privacy policy change:



Dialog that appears when users click "more options:"

Choose what's right for you

Need more info first?
[Learn more about these features](#)

- No changes – continue on your way**
We won't change anything. Your Google experience – including the ads you see – will remain the same.
- No changes – review key privacy settings in more detail**
Take the *Privacy Checkup* to review key settings, including settings for ads.
- Yes, I agree – turn on these new features**
You can change your mind any time in *My Account*

[BACK](#) [DONE](#)

Appendix C

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

Privacy and Terms

By choosing "I agree" below you agree to Google's [Terms of Service](#).

You also agree to our [Privacy Policy](#), which describes how we process your information, including these key points:

Data we process when you use Google

- When you use Google services to do things like write a message in Gmail or comment on a YouTube video, we store the information you create.
- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity – including information like the video you watched, device IDs, IP addresses, cookie data, and location.
- We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.

CANCEL

I AGREE

Appendix E

Combining data

We also combine data among our services and across your devices for these purposes. For example, we show you ads based on information from your use of Search and Gmail, and we use data from trillions of search queries to build spell-correction models that we use across all of our services.

CANCEL

I AGREE