Before the
Federal Trade Commission
Washington, DC

In the Matter of	)
	)
Google Inc.	)
	)
	)

Complaint, Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center (EPIC)

I. Introduction

1. This complaint concerns "Store Sales Measurement," a consumer profiling technique pursued by the world's largest Internet company to track consumers who make offline purchases. Google has collected billions of credit card transactions, containing personal customer information, from credit card companies, data brokers, and others and has linked those records with the activities of Internet users, including product searches and location searches. This data reveals sensitive information about consumer purchases, health, and private lives. According to Google, it can track about 70% of credit and debit card transactions in the United States.

2. Google claims that it can preserve consumer privacy while correlating advertising impressions with store purchases, but Google refuses to reveal—or allow independent testing of— the technique that would make this possible. The privacy of millions of consumers thus depends on a secret, proprietary algorithm. And although Google claims that consumers can opt out of being tracked, the process is burdensome, opaque, and misleading.

3. Google's reliance on a secret, proprietary algorithm for assurances of consumer privacy, Google's collection of massive numbers of credit card records through unidentified "third-party partnerships," and Google's use of an opaque and misleading "opt-out" mechanism are unfair and deceptive trade practices subject to investigation and injunction by the FTC.

II. Parties

4. The Electronic Privacy Information Center ("EPIC") is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of

consumers.[1] EPIC's complaint concerning Google Buzz provided the basis for the Commission's investigation and subsequent settlement concerning the social networking service.[2] Following EPIC's complaint, the FTC successfully petitioned a federal court for a permanent injunction barring sales of CyberSpy's "stalker spyware," over-the-counter surveillance technology allowing individuals to spy on other individuals.[3] EPIC also filed a consumer complaint with the Commission, alleging that AskEraser falsely represented that search queries would be deleted when in fact they were retained by the company and made available to law enforcement agencies.[4]

5. Google, Inc., was founded in 1998 and is based in Mountain View, California. Google's headquarters are located at 1600 Amphitheatre Parkway, Mountain View, CA 94043. At all times material to this complaint, Google's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

6. Google is expected to command nearly 41 percent of the $83 billion Internet advertising market in the United States this year. "And some analysts say that advertisers are clamoring for an alternative to the two giant Internet platforms who dominate the industry."[5]

III. Factual Background

A. Google Is Tracking When Consumers Who See Ads Make Purchases in Stores

7. Store Sales Measurement attempts to measure in-store revenue for consumer purchases resulting from advertising purchased from Google, the largest advertising company in the world. This technique works with other Google advertising techniques, such AdWords,

---

[1] *See, e.g.*, Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[2] Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched."). The Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."

[3] *FTC v. CyberSpy Software*, LLC, No. 6:08-cv-1872-Orl-31GJK, 2009 WL 2386137 (M.D. Fla. July 31, 2009) (Order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/06/100602cyberspystip.pdf.

[4] EPIC: Does AskEraser Really Erase?, https://epic.org/privacy/ask/.

[5] Hamza Shaban, *Quarterly earnings for Google, Facebook reflect growing dominance in digital ad market*, Washington Post (July 27, 2017), https://www.washingtonpost.com/business/economy/quarterly-earnings-for-google-facebook-reflect-growing-dominance-in-digital-ad-market/2017/07/27/938360e4-731a-11e7-8f39-eeb7d3a2d304_story.html.

Google Analytics, and DoubleClick Search, in the Google Attribution advertising tracking suite.[6]

8. The technique correlates in-store purchases with actions users take on their smartphones using Google's Internet-based services, such as searching for products or searching for alternative locations to make purchases.[7]

9. Google has "begun using billions of credit card transaction records . . . even when they happen offline[.]"[8]

10. Google collects credit card transaction information from direct import of customer data by advertising clients, through "third-party partnerships, which capture approximately 70% of credit and debit card transactions in the United States,"[9] and through "data licensing agreements with major credit card companies."[10]

11. A "third-party data partner" matches information in a customer relationship manager ("CRM") system to clicks on AdWords ads. Data is then imported into AdWords to track "which keywords, ads, ad groups, and campaigns likely have the greatest impact on store sales."[11]

12. Google tracks customers through "data driven attribution, which uses machine learning to analyze sales or conversion data and calculate the actual contribution of each step the consumer takes."[12]

13. The technique is available to large advertisers with multiple physical stores that are tracking store sales data in a CRM system.[13] The technique is currently deployed in the United States.[14]

14. Google has released few details about how its algorithm is supposed to protect private consumer information, such as names, credit card numbers, and purchase information.

---

[6] Google, *Powering Ads and Analytics Innovation with Machine Learning*, Inside AdWords (May 23, 2017), https://adwords.googleblog.com/2017/05/powering-ads-and-analytics-innovations.html.

[7] Liam Tung, *Google: We'll Track Your Offline Credit Card Use to Show That Online Ads Work*, ZDNet (May 24, 2017), http://www.zdnet.com/article/google-well-track-your-offline-credit-card-use-to-show-that-online-ads-work/.

[8] Elizabeth Dwoskin & Craig Timberg, *Google Now Knows When Its Users Go to the Store and Buy Stuff*, Wash. Post (May 23, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/.

[9] Google, *Powering Ads and Analytics Innovation with Machine Learning*, *supra* note 6.

[10] Greg Sterling, *YouTube Location Extensions, In-Store Sales Measurement Now Available*, Marketing Land (May 23, 2017), http://marketingland.com/google-next-youtube-location-extensions-store-sales-measurement-now-available-215618.

[11] Google, *Track Store Sales Conversions with a Data Partner*, AdWords Help, https://support.google.com/adwords/answer/6361305.

[12] Robert Hof, *Did That Ad Work? Google Debuts New AI-Driven Attribution Service*, Forbes (May 23, 2017), https://www.forbes.com/sites/roberthof/2017/05/23/did-that-ad-work-google-debuts-new-ai-driven-ad-attribution-service/.

[13] Google, *Track Store Sales Conversions with a Data Partner*, supra note 11.

[14] Sterling, *supra* note 10.

The Washington Post reports that "mathematical formulas convert people's names and other purchase information, including the time stamp, location, and the amount of the purchase, into anonymous strings of numbers."[15]

15. Google tells its advertising clients there is no "need to share any customer information" because all data will be "aggregated and anonymized" and data will be reported in a "secure and privacy safe way."[16]

16. Google said it would not handle payment records directly, instead using "double blind matching" between payment data and Google user data. Google's proprietary algorithm reportedly converts people's names and other purchase information, such as "the time stamp, location, and the amount of the purchase," into "anonymous strings of numbers."[17]

17. Google claims that is unable to release details about the algorithm because of a pending patent application. But Google has revealed that the algorithm is based on CryptDB, described in a 2011 MIT research paper funded by Google and Citigroup.[18]

18. The foundational algorithm on which the Google algorithm is based has known security flaws. In 2015, researchers were able to hack into a CryptDB protected database of healthcare records and access over 50% (sometimes 100%) of sensitive patient data at an individual level.[19]

19. Google provided no further detail on how these vague promises will be carried out and does not detail how the system works or what companies are analyzing the records.[20]

20. Google "would not say" whether customers have consented to the use of their data to tie purchases to advertising and other actions.[21]

21. Fair Isaac estimates that in 2016 approximately 77% of the US population, or 248 million people, had a credit card.[22] Mastercard and Visa report a total of 654 million debit cards in the United States in 2015.[23] If Google's algorithm does not work as described, Google

---

[15] Dwoskin & Timberg, *supra* note 8.

[16] Google, *Powering Ads and Analytics Innovation with Machine Learning*, *supra* note 6.

[17] Dwoskin & Timberg, *supra* note 8.

[18] *Id.*

[19] Sean Gallagher, *MS Researchers Claim To Crack Encrypted Database with Old Simple Trick*, Ars Technica (Sep. 4, 2015), https://arstechnica.com/security/2015/09/ms-researchers-claim-to-crack-encrypted-database-with-old-simple-trick/

[20] Dwoskin & Timberg, *supra* note 8.

[21] *Id.*

[22] Fair Isaac Corp., *The Digital Generation* (2016), available at http://www.creditcards.com/credit-card-news/assets/FICO-the-digital-generation-are-millenials-looking.pdf.

[23] Visa, *Operational Performance Data* (2015), https://s1.q4cdn.com/050606653/files/doc_financials/2015/Visa-Inc-2015-Operational-Performance-Data.pdf; MasterCard, *Supplemental Operational Performance Data* (2015), http://s2.q4cdn.com/242125233/files/doc_financials/supplemental/2015/2Q15-MA-Supplemental-Operational-Performance-Data.pdf

could risk the exposure of credit card transactions and other private information of millions of U.S. consumers.

B. Store Sales Measurement is a Continuation of Google's Efforts to Track Advertising to Store Purchases.

22. In 2014 Google launched Store Visit Management, which allows AdWords advertisers to track how many customers click on a search or display ads and then subsequently visit their stores.[24] Large advertisers, such as Home Depot, Nissan, and Sephora, have used the product[25] and Google claims over 5 billion store visits have been measured by AdWords customers to date.[26]

23. Store Visit Management attempts to measure a subset of Google users who have opted into location history tracking, clicked on an ad, and subsequently visited a specific store. An algorithm extrapolates that data to non-signed in users who exhibit the same behavior to give advertisers an accurate estimate of how many customers visit their stores after interacting with their AdWords ads.[27] The accuracy of the data and extrapolations is verified with panel surveys.[28]

24. Google claims that all data is anonymized and aggregated to protect user privacy.[29] Additionally, Google claims that users can delete and/or opt out of location history tracking on both Android and iPhone devices if they do not want to be tracked:

---

[24] Google, *Measure More: Improving Estimated Total Conversions with Store Visit Insights*, Inside AdWords Blog (Dec. 18, 2014), https://adwords.googleblog.com/2014/12/measure-more-improving-estimated-total.html.
[25] Dwoskin & Timberg, *supra* note 8..
[26] Google, *Powering Ads and Analytics Innovation with Machine Learning*, *supra* note 6.
[27] Google Small Businesses, AdWords Store Visits Conversion video, :27-:40 (Apr. 8, 2015), https://www.youtube.com/watch?v=qqAz09YcN3E.
[28] Matt Lawson, *Under the Hood: How Google AdWords Measures Store Visits*, Search Engine Land (Jun. 18, 2015 10:28AM), http://searchengineland.com/hood-google-adwords-measures-store-visits-222905.
[29] *Id.*

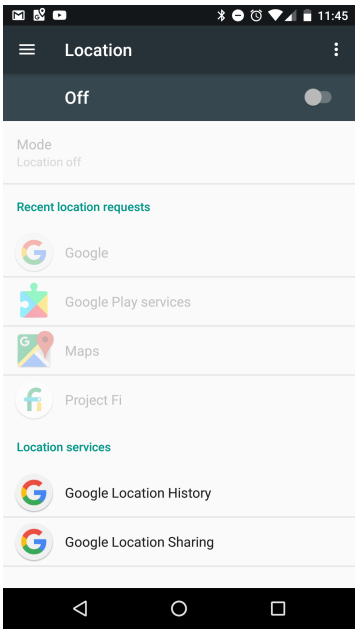

Figure 1: User Location History Opt in/Opt Out Controls on Android Devices

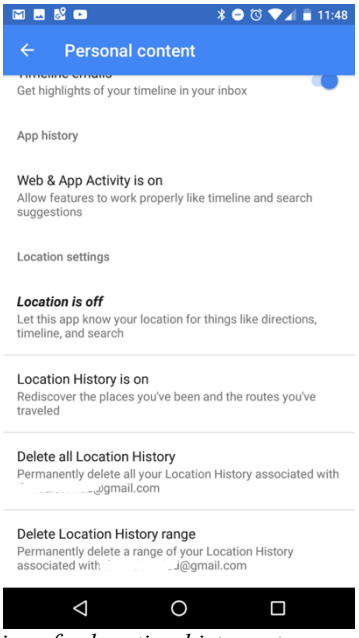

Figure 2: User settings for location history storage on Android Devices

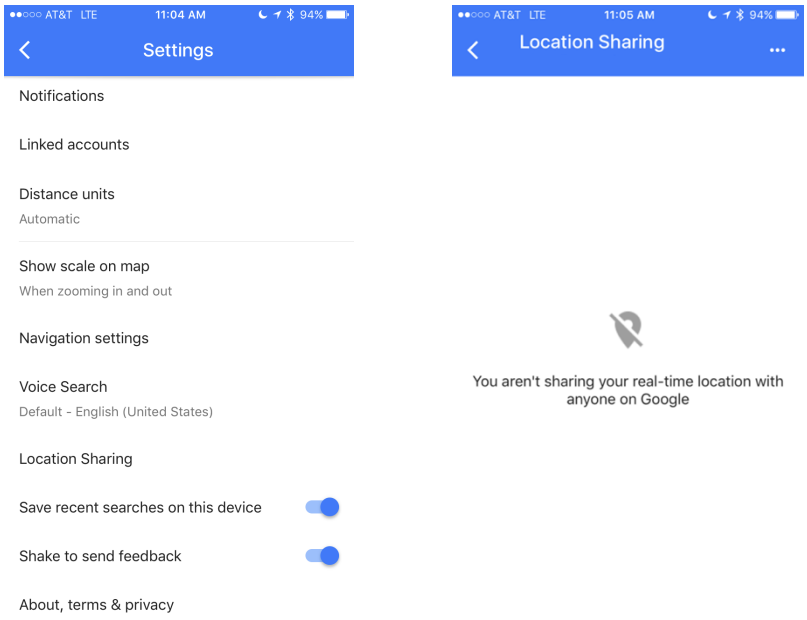

Figure 3: User settings for location sharing in Google Maps on iPhone 6

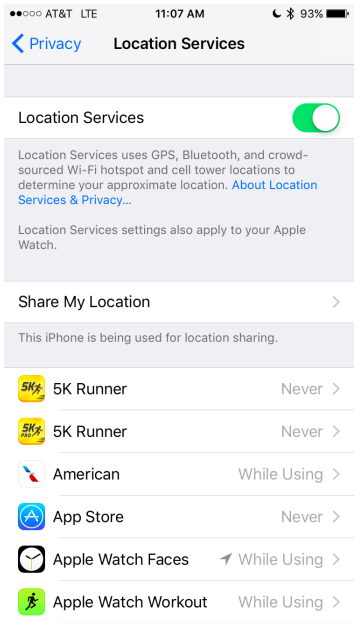

Figure 4: User Settings for Over Location Sharing on iPhone 6 Device Settings

25. In March 2017, Google announced it would expand the availability of Store Visit Conversions to AdWords customers who buy YouTube TrueView Ads.[30] Google also announced an update to the machine learning algorithm that measures store visits. In Google's words: "We're now able to train on larger data sets and increase our accuracy in prioritizing which location signals are most predictive of true visits. This allows us to reliably measure more store visits in contexts that are typically tricky, such as in multi-

[30] Google, *New Measurement Innovations Unlock More Store Visits Data*, Inside AdWords (Mar. 29, 2017), https://adwords.googleblog.com/2017/03/new-measurement-innovations-unlock-more.html.

story malls and dense geographies where many business locations are situated close to each other."[31]

26. Google AdWords also allows advertisers to import offline conversions into the AdWords user interface to enable streamlined advertising spend attribution. These include offline sales, offline lead conversions, signing a contract, and any tracking included in a consumer owned Consumer Relationship Manager (CRM) system.[32]

27. To import a generic offline conversion, AdWords provides advertisers with a unique ID, called a GCLID, for every click that comes to their website from an AdWords ad. Advertisers save that ID along with whatever lead information they collect from the person who clicked their ad. Later, when that person "converts" in the offline world, the advertiser gives that GCLID back to AdWords along with a few details about the type of conversion it was and when it happened. Then AdWords records this conversion along with other conversion tracking data.[33]

28. Advertisers can directly import offline conversions for any of the lead status or opportunity stages recorded Salesforce Sales Cloud. As Google tells its advertising clients:

> When someone clicks your ad and goes to your website, the website captures a . . . "GCLID" . . . and stores it in a cookie. AdWords uses this ID to determine which click on which ad gets credit for any future conversions. When the customer submits a lead form on your website, your website will pass along the GCLID to Salesforce and stores it within the corresponding lead and any future opportunities that are derived from this lead.[34]

29. To import other conversions, including in store sales, from customer owned CRM databases, a "third-party data partner will match the sales information [advertisers] track in a CRM to clicks on [their] AdWords ads. This data will then be imported into AdWords, so [they] can see which keywords, ads, ad groups, and campaigns likely have the greatest impact on store sales."[35] This method of in-store conversion tracking continues to be available in the newly announced product.

---

[31] *Id.*
[32] Google, *About Offline Conversion Tracking*, AdWords Help, https://support.google.com/adwords/answer/2998031.
[33] *Id.*
[34] Google, *About AdWords Conversion Import for Salesforce*, AdWords Help, https://support.google.com/adwords/answer/6179720.
[35] Google, *Track Store Sales Conversions with a Data Partner*, AdWords Help, https://support.google.com/adwords/answer/6361305.

30. Google began testing in-store sales conversion tracking in 2014.[36] Google partnered with Acxiom and Datalogix to get credit card transaction data for this initial beta test.[37] This initial test reportedly worked "by matching anonymous cookies on users' computers to the in-store sales info gathered by the data providers."[38]

C. Secret, Proprietary Algorithms Fail to Protect Sensitive Personal Information

31. In January 2016, the FTC recognized that the use of a proprietary algorithm that did not sufficiently or effectively encrypt personal data. Henry Schein Practice Solutions, a dental software firm, paid $250,000 to settle charges from the FTC that it "falsely advertised the level of encryption it provided to protect patient data."[39] Henry Schein repeatedly made claims that its dentistry software, *Dentrix G5*, encrypted patients' personal data effectively. This personal data included instances of patients' Social Security Number, driver's license number, and prescriptions.[40]

32. Professor Latanya Sweeney and Ji Su Yoo at Harvard University were able to de-anonymize a dataset that included prescription data associated with encrypted Resident Registration Numbers (RRNs), South Korea's National Identifiers.[41] This de-anonymization was made easier because the RRN string of digits are not randomly selected. Credit card numbers are also often not randomly selected strings of digits. Credit card numbers contain prefixes that reference the issuer of the card and "check digits" which are suffix digits calculated from the preceding numbers.[42]

33. In 2014, after an EPIC complaint,[43] the FTC reached a settlement with Snapchat.[44] Snapchat had promised that its secret, proprietary algorithms would make images sent in its app "disappear forever."[45]

D. Google's Refusal to Reveal its Partnership with Data Brokers Further Endangers Consumer Privacy

34. Google has not released the identity of the "third party partnerships" that allow them access to "approximately 70% of credit and debit card transactions in the US."[46]

---

[36] Ginny Marvin, *Report: Google Running Another Test to Map In-Store Sales to Adwords Ads*, Search Engine Land (Apr. 12, 2014, 9:45pm), http://searchengineland.com/report-google-running-another-test-map-store-sales-adwords-ads-188986.
[37] *Id.*
[38] *Id.*
[39] FTC Approves Final Order in Henry Schein Practice Solutions Case, FTC.gov (2016), https://www.ftc.gov/news-events/press-releases/2016/05/ftc-approves-final-order-henry-schein-practice-solutions-case.
[40] https://www.ftc.gov/system/files/documents/cases/160105scheincmpt.pdf.
[41] Latanya Sweeney & Ji Su Yoo, *De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data*, Technology Science, 2015092901 (Sept. 29, 2015), https://techscience.org/a/2015092901.
[42] *Credit Card Validation - Check Digits,* Electrical Engineering and Computer Science University of Michigan, https://web.eecs.umich.edu/~bartlett/credit_card_number.html (last visited Jun. 30, 2017).
[43] EPIC, *In re: Snapchat*, https://epic.org/privacy/internet/ftc/snapchat/.
[44] Decision and Order, *In re* Snapchat Inc., F.T.C. Docket No. C-4501 (Dec. 23, 2014).
[45] EPIC, *In re: Snapchat*, https://epic.org/privacy/internet/ftc/snapchat/.

35. The information Google needs is likely to come from data brokers—companies that collect information of individuals from government sources, publicly available sources, and commercial data sources.[47] Data brokers collect a wide range of information, some of which may include very personal information. Some information collected by data brokers may be false or outdated. Consumers have no ability to correct this information.[48] In a report dated May 2014, FTC called for legislative action to regulate data brokers.[49] But no such regulations have been established.

36. Data brokerage is a crowded space with many companies potentially working with Google on this project. The issues associated with varying levels of ease of access and effectiveness of each company's process and the lack of permanent and full data deletion are exacerbated by the uncertainty surrounding the identity of companies partnering with Google for this project. This presents an unsatisfactory, unreasonable and unfair situation for the consumer and their ability to control the protection of their personal data.

37. Data brokerages are obvious targets for hackers, and are often successfully breached. Epsilon, a data brokerage that handles more than 40 billion emails annually, was hacked in 2011. Three of the top ten American banks were affected. It was later found that no PII was obtained, but the emails breached could be used for phishing attacks and spam.[50] Experian, one of the largest data brokers in the world, revealed in October 2015 that it had been breached, compromising the personal information of 15 million people.[51] In 2013, LexisNexis, Dun & Bradstreet, and Kroll Background America, three major data brokerages, were breached by a group of hackers specializing in the selling of social security numbers.[52]

38. Most data brokers store consumer information indefinitely, even when such information is later updated.[53] Therefore, data brokers have a record of consumers' changes over time. If unscrupulous actors obtain this record, they will have a clear picture of consumers' habits, enabling them to predict passwords and other authentication credentials.

39. Data brokers offer little to no consumer choice on the handling of their data. Data brokerages rarely offer consumers the choice to opt out.[54] These companies are generally

---

[46] BBC, *Google plans to track credit card spending*, BBC *(*May 26, 2017), http://www.bbc.com/news/technology-40027706.

[47] Federal Trade Commission, *Data Brokers; A Call for Transparency and Accountability* (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[48] *Id.*

[49] *Id.*

[50] Josh Halliday, *Epsilon Email Hack: Millions of Customers' Details Stolen* (Apr. 2, 2011), https://www.theguardian.com/technology/2011/apr/04/epsilon-email-hack.

[51] Sam Thielman, *Experian Hack Exposes 15 Million People's Personal Information* (Oct. 1, 2015), https://www.theguardian.com/business/2015/oct/01/experian-hack-t-mobile-credit-checks-personal-information.

[52] Kreb on Security, *Data Broker Giants Hacked by ID Theft Service* (Sept. 25, 2013), https://krebsonsecurity.com/tag/kroll-background-america-inc/.

[53] *Id*.

[54] *Id*.

not consumer-facing and receive no oversight from government departments. Even when such choices are offered, the consumer has little idea as to whether their wish was truly followed.[55] In addition, data brokers' opt-out options do not clearly define whether the consumer is able to opt out on all uses of his or her data.[56] Therefore, consumers may try to opt out but remain unaware on the true limitations of the uses of their data.

40. In short, consumers have no control over their information and where it goes; their own information may be used for extortion against them without them knowing it. Consumers have no clear way to stop receiving advertisements, or to stop the spread of their expired or false information even when they choose to opt out.

41. Some companies in this industry have been officially and unofficially tied to Google. The Wall Street Journal and other news outlets have cited both Acxiom and Datalogix as companies with the capabilities to partner with Google in this project.[57] LiveRamp Inc., an Acxiom company, is described as "a firm that helps match offline data about customers with online information"[58]. Its website also lists Google advertising and marketing subsidiaries as partners including Google AdWords, Google Analytics 360 Suite, Google Customer Match, Google Display Network, DoubleClick Bid Manager, and DoubleClick Search.[59]

E. Internet Users Cannot Effectively Avoid Google's Intrusive Tracking

42. Internet users, the vast majority of whom must have a Google account to access email and other essential Internet services, have no effective way to opt out of Google's new technique for tracking off-line behavior.

43. According to Google, turning off Web & App Activity stops Google from saving information about the ads a user clicks.[60] However, serve and click data may still be stored in a manner that allows for personal identification of the user even when Web & App Activity is turned off. Whenever an ad is served to a user's browser, Google's servers create a log that includes the user's IP address and a unique identifier attached to the relevant Google advertising cookie.[61]

44. Google also uses cookies to log when a user clicks on an ad.[62] Google claims that it "anonymizes" the server logs by removing part of the IP address in the log after nine

---

[55] David Lazarus, *Who oversees data brokers selling your personal info? No one* (Oct. 26, 2016), http://www.latimes.com/business/lazarus/la-fi-lazarus-list-brokers-20161028-snap-story.html.
[56] Julia Angwin, *Privacy Tools: Opting Out from Data Brokers* (Jan. 30, 2014), https://www.propublica.org/article/privacy-tools-opting-out-from-data-brokers.
[57] Alistair Barr, *Google Says New Store Data Help Mobile Ads*, The Wall Street Journal (May 21, 2015), https://www.wsj.com/articles/google-touts-mobile-ad-technology-1432220552
[58] *Getting to Know You*, The Economist (Sept. 11, 2014), http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party
[59] Liveramp, *Partners*, https://liveramp.com/partners/.
[60] Google, *See and Control Your Search Activity*, https://support.google.com/websearch/answer/54068.
[61] Google, *Privacy & Terms: Advertising*, https://www.google.com/intl/en/policies/technologies/ads/.
[62] Google, *Privacy & Terms: Advertising*, https://www.google.com/intl/en/policies/technologies/ads/.

months, and removing the cookie information after eighteen months.[63] Turning off ad personalization and/or opting out of Google cookies does not prevent ads from being served to a user,[64] and these serves continue to be logged on the server, along with the user's IP address. There is no way for a user to prevent Google from logging their IP address when an ad is served without using a third party product, such as a Virtual Private Network (VPN).

45. Information about whether Google stores information about the ads a user clicks is buried several pages into Google's privacy controls. The information eventually provided on those pages does not disclose the extent to which opting out of Web & App Activity stops Google from tracking a user's interactions with Google ads:

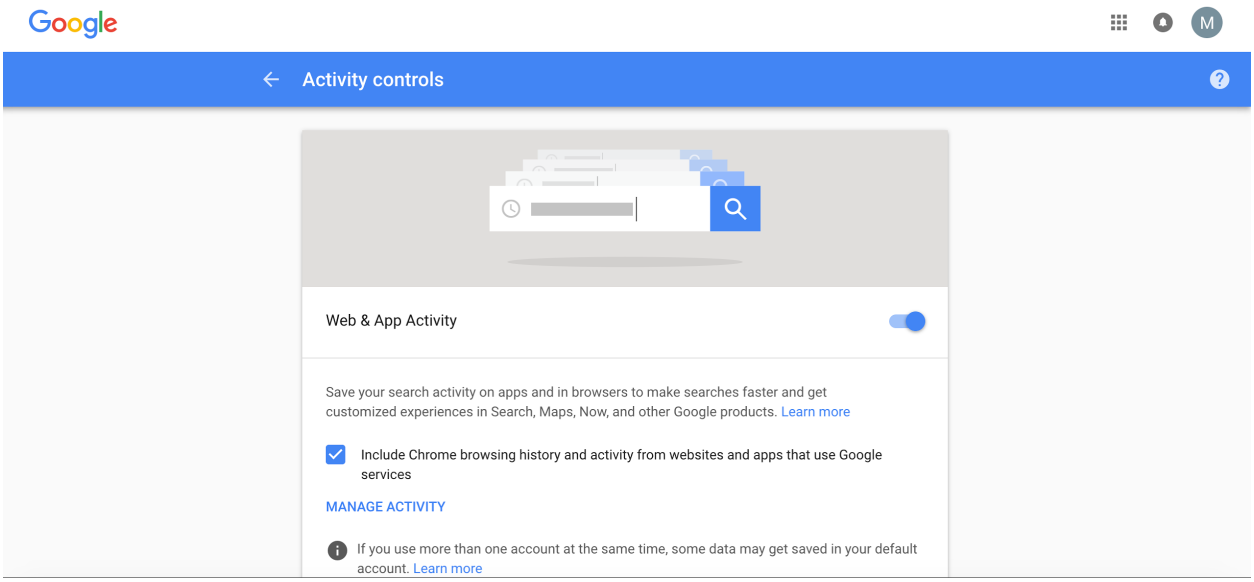

Figure 5: The Web & App Activity setting control. To discover that this setting controls whether Google stores information about a user's ad clicks, the user must click on the first "Learn more" link.

[63] *Id.*

[64] Google, *Opt Out Of Seeing Personalized Ads*, https://support.google.com/ads/answer/2662922.

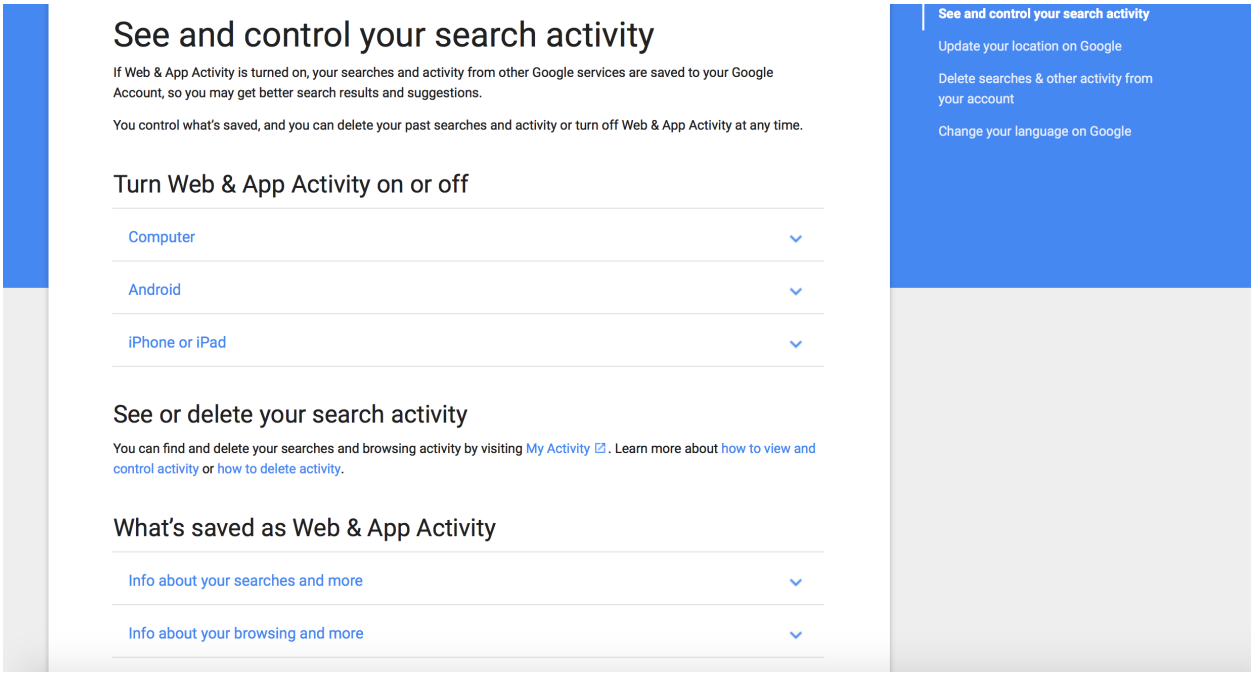

Figure 6: Once on the "Learn more" page, a user must expand the "Info about your searches and more" section.

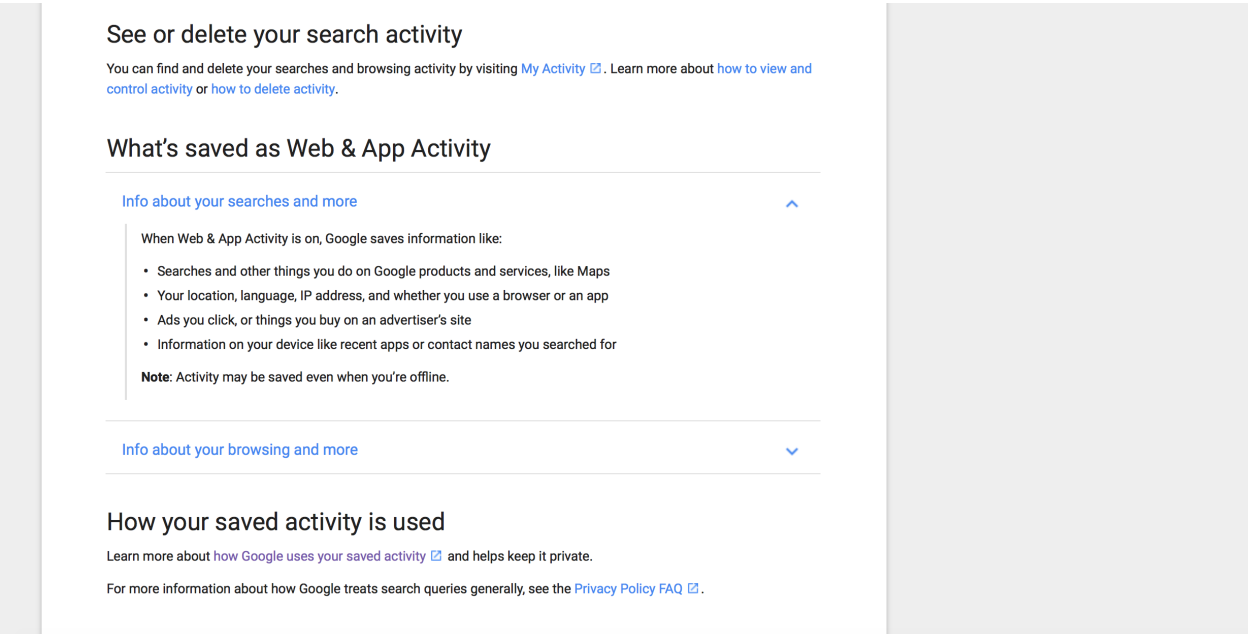

Figure 7: The first statement that the Web & Activity setting controls whether Google can save information about the ads a user clicks.

46. Tracking of Web & App Activity and Chrome browsing history is enabled default for new, non-organizational Google users.[65]

47. Disabling Google's Ad Personalization setting only stops Google from serving a user personalized ads while signed in to his or her Google account.[66]

[65] Google, *G Suite Administrator Help: Turn Web History On or Off*, https://support.google.com/a/answer/6304876.

48. To disable Google ad cookies, which follow users to third party sites and are active even when users are signed out of their Google accounts, a user must click on the "Visit AdChoices" icon at the bottom of the Ad Personalization page.[67] That brings the user to a third party site belonging to Digital Advertising Alliance, where he or she may opt out of a wide variety of ad tracking cookies, including Google's.[68] Opting out of a tracking cookie requires downloading an opt-out cookie for each browser an individual uses.[69] Clearing a browser's cookies deletes the opt-out cookie, which re-enables tracking.[70] The Digital Advertising Alliance offers an extension to remember a user's opt out preferences, which is only available for Internet Explorer, Firefox, and Google Chrome.[71]

49. To permanently disable Google DoubleClick cookies, users must scroll to the bottom of the Ad Personalization page and click a link to install a DoubleClick opt out browser extension.[72] The extension is only available for Internet Explorer, Firefox, and Google Chrome.[73]

50. Users can also block all cookies in each of the browsers they use and across their devices, or browse in incognito mode, to avoid Google's ad cookies. However, blocking all cookies will interfere with the functionality of many web sites.

51. When a user creates a Google account, Google requires the user to accept its privacy policy. In the pop-up that prompts acceptance, Google states that it processes data, such as a user's IP address, for "Google services like ads." Google claims that the user "can control how we collect and use this data at My Account." But there does not appear to be a way to prevent Google from matching user data to credit card transaction data held by a third party.

---

[66] Google, *Opt Out Of Seeing Personalized Ads*, supra note 64.

[67] Google, *Ads Personalization*, https://www.google.com/settings/u/0/ads/authenticated#fyRr4c.

[68] Digital Advertising Alliance, *WebChoices: Digital Advertising Alliance's Consumer Choice Tool for Web (Beta)*, http://optout.aboutads.info/#!/.

[69] Digital Advertising Alliance, *Frequently Asked Questions about the Digital Advertising Alliance and its Consumer Choice Tools*, http://www.aboutads.info/how-interest-based-ads-work#cookies-and-optout.

[70] *Id.*

[71] Digital Advertising Alliance, *Protect My Choices for Chrome, Firefox, and Internet Explorer*, http://www.aboutads.info/PMC.

[72] Google, *Ads Personalization*, supra note 67.

[73] Google, *Ad Settings: Opting Out Permanently: Browser Instructions*, https://www.google.com/settings/u/0/ads/plugin.

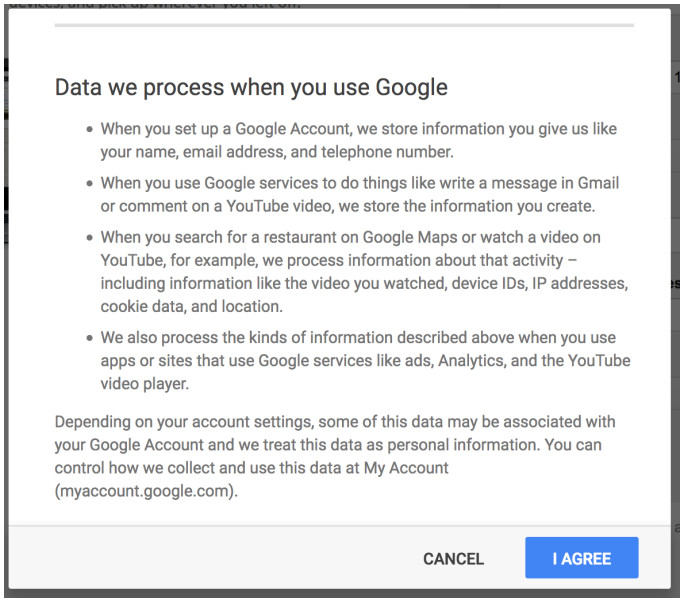

Figure 8: Pop-up window seeking user consent to Google's privacy policy at sign-up.

52. Google's Privacy Policy states that Google uses "information collected from cookies and other technologies, like pixel tags, to improve … the overall quality of our services."[74] Google also states that it "may combine personal information from one service with information, including personal information, from other Google services."[75] Further, the policy states "[d]epending 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."[76] Finally, the policy states that Google "will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy."[77]

F. Consumers Object to Online-to-Offline Tracking

53. Regarding Google's effort to track offline behavior, Professor Niraj Dawar wrote in the *Harvard Business Review*:

> Google has a more complete picture of the consumer than any other company, because it knows when consumers view ads in Google Search, Gmail, YouTube, Google Maps, and Android apps. It also knows where consumers go, both online and in the physical world, based on cookies and location data from their phones. But the online giant has not had a very

[74] Google, *Privacy Policy: How We Use Information We Collect*, https://www.google.com/intl/en/policies/privacy/#infouse.
[75] *Id.*
[76] *Id.*
[77] *Id.*

> clear picture of where consumers shop in the physical world and how much they spend — until now.[78]

54. Paul Stephens of Privacy Rights Clearinghouse said in a statement to the *Washington Post*, "What we have learned is that it's extremely difficult to anonymize data. If you care about your privacy, you definitely need to be concerned."[79]

55. Renate Samson from Big Brother Watch explained to *BBC*, "The one thing people regularly state as 'creepy' online is when an advert follows them around the internet. These plans appear to extend 'creepy' into the physical world."[80]

56. Some commenters to a *Washington Post* article about Google's plans expressed concerns over their privacy and security of their data while some others expressed resignation to the status quo.[81]

    a. Commenter "z0rr0" said, "We need a law that lets us 'monetize' ourselves. A penny for each use of our data. Why should we be the only ones who don't profit from our own lives?"[82]

    b. Commenter "Jake Holman" said, "Look, the 'battle for privacy' is pretty much over. I mean, the FBI could announce to the American people that each new cellphone contains built-in spyware which allows them to record every call, message, and tweet, and about three-quarters of the people wouldn't care."[83]

    c. Commenter "PaulS2" asked, "Is there a way to opt-out?"[84] To which commenter Col Forbin responded, "Not one that doesn't involve pall-bearers, I fear."[85]

---

[78] Niraj Dawar, *Has Google Finally Proven That Online Ads Cause Offline Purchases?*, Harvard Business Review (Jun. 1, 2017), https://hbr.org/2017/06/has-google-finally-proven-that-online-ads-cause-offline-purchases.

[79] Dwoskin & Timberg, *supra* note 8.

[80] BBC, *Google Plans To Track Credit Card Spending*, BBC (May 26, 2017), http://www.bbc.com/news/technology-40027706.

[81] Dwoskin & Timberg, *supra* note 8.

[82] "z0rr0," Comment to Elizabeth Dwoskin & Craig Timberg, *Google Now Knows When Its Users Go to the Store and Buy Stuff*, Wash. Post (May 25, 2017, 11:34 AM), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?commentID=washingtonpost.com/ECHO/item/8fe1d63c-5234-418d-9276-a8634ea210eb&outputType=comment.

[83] "Jake Holman," Comment to Elizabeth Dwoskin & Craig Timberg, *Google Now Knows When Its Users Go to the Store and Buy Stuff*, Wash. Post (May 26, 2017 03:50 AM), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?commentID=washingtonpost.com/ECHO/item/47655b3c-53bc-4dab-88d7-826d475d3791&outputType=comment.

[84] "PaulS2," Comment to Elizabeth Dwoskin & Craig Timberg, *Google Now Knows When Its Users Go to the Store and Buy Stuff,* Wash. Post (May 25, 2017 09:24 AM), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?commentID=washingtonpost.com/ECHO/item/ca89df9b-f57e-4cf8-b31b-4cfe968f120a&outputType=comment.

d. Commenter "FishyBulb" posted:

> I don't oppose advertising, or being advertised to. Everyone's got to make money, right? The reason I use adblockers, script blockers, encryption services and the like is because this goes beyond advertising. A billboard or simple banner ad is advertising. The highly targeted form of advertising that Google and Facebook use is stalking, and I oppose every effort to perpetuate it.
>
> On top of that, I think it's clear that all of this information is highly vulnerable to attack and theft, and I don't doubt for a minute that the level of information collected on an individual could be traced right back to them, no matter how these companies claim to anonymize the data. These companies not only know every single bit of information about you, they can also assume your psychology, your habits and anything else to create a profile of you that is far beyond what you know about yourself. It's creepy, intrusive and wrong.[86]

e. In response to "FishyBulb," commenter "Comma Chameleon" said:

> There are lots of compelling reasons to use an ad blocker. Many online ads are seriously obnoxious. They flash and bounce around and break up the page in distracting ways (which I realize is often intentional). They use up valuable mobile resources like cellular data and smartphone computing power. One time I was even attacked by malware on a fairly reputable sports news site. I think one of the big challenges for site designers and the ad industry generally is to try to make ads that capture people's attention but do so with a minimum of disturbance -- and hopefully respecting people's privacy as well, because you're right, it does kind of feel like stalking. It's creepy.[87]

---

[85] "Col Forbin," Comment to Elizabeth Dwoskin & Craig Timberg, *Google now knows when its users go to the store and buy stuff*, Wash. Post (May 25, 2017 04:48 PM), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?commentID=washingtonpost.com/ECHO/item/ca89df9b-f57e-4cf8-b31b-4cfe968f120a&outputType=comment.

[86] "FishyBulb," Comment to Elizabeth Dwoskin & Craig Timberg, *Google now knows when its users go to the store and buy stuff*, Wash. Post (May 23, 2017, 01:06 PM), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?commentID=washingtonpost.com/ECHO/item/4ae47726-037f-4edb-8c5e-c5c4f7377cfe&outputType=comment.

[87] "Comma Chameleon," Comment to Elizabeth Dwoskin & Craig Timberg, *Google now knows when its users go to the store and buy stuff*, Wash. Post (May 23, 2017, 11:35 PM), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?commentID=washingtonpost.com/ECHO/item/4ae47726-037f-4edb-8c5e-c5c4f7377cfe&outputType=comment.

f. Commenter TwoFeetThick posted, "I'm thinking we need some new laws to protect privacy. Hey Congress, are you paying attention? How about you do something that actually benefits normal Americans for a change?"[88]

g. Commenter Natalie Jones, wrote, "We need to focus regulation on protecting identifiable consumer data from being shared because that's really all we can do at this point."[89]

G. Algorithms that Track Consumer Behavior Must Be Transparent

57. Algorithmic transparency is essential to protecting consumers' rights.[90]

58. Algorithmic transparency is the basis of accountability for automated-decisionmaking.[91]

59. The code should be open.[92]

60. There should be no secret profiling.[93]

H. EPIC Warned the FTC of the Threat to Privacy, Innovation, and Competition Posed by Google's Attempt to Link the Online and Offline Activities of Consumers

61. In 2000, EPIC filed a complaint with the FTC opposing the merger of DoubleClick, an advertising company now owned by Google, with Abacus Direct, the country's largest catalog database firm at the time. The complaint alleged the DoubleClick was unlawfully tracking online activity to an offline database of customers' identified purchases.[94] DoubleClick eventually dropped its plan to track Internet users.[95]

---

[88] "TwoFeetThick," Comment to Elizabeth Dwoskin & Craig Timberg, *Google now knows when its users go to the store and buy stuff*, Wash. Post (May 23, 2017, 10:30 AM [Edited]), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?commentID=washingtonpost.com/ECHO/item/237351c1-0abf-480a-ae3f-7efd20718ba7&outputType=comment.

[89] "Natalie Jones," Comment to Elizabeth Dwoskin & Craig Timberg, *Google now knows when its users go to the store and buy stuff*, Wash. Post (May 24, 2017, 09:28 AM), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?commentID=washingtonpost.com/ECHO/item/52926192-7fd2-4153-a39a-dbe4323aeff5&outputType=comment.

[90] *See* Danielle Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 8 (2014) ("transparency of scoring systems is essential"); Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (2015).

[91] See 14 C.F.R. § 255.4 (requiring transparency for reservation system display information); Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 Northwestern L. Rev. 105 (2010).

[92] EPIC, *Algorithmic Transparency*, https://epic.org/algorithmic-transparency/

[93] *Id.*

[94] Complaint and Request for Injunction, Request for Investigation and for Other Relief, *In re* DoubleClick, Inc. (Feb. 10, 2000), https://epic.org/privacy/internet/ftc/DCLK_complaint.pdf. *See also* EPIC, *Double Trouble*, https://epic.org/privacy/doubletrouble/,

[95] Will Rodger, *DoubleClick Backs off Web-tracking Plan*, USA Today (Mar. 2, 2000), http://web.archive.org/web/20000517132836/http://www.usatoday.com/life/cyber/tech/cth486.htm.

62. In 2007, Google announced that it would acquire DoubleClick.[96] Both companies were leading figures in the online advertising industry, DoubleClick in ad serving and Google in sponsored searches, and through its product AdSense, in contextual advertising.[97] The underlying AdSense and DoubleClick business models both substantially depend on tracking users' preferences to increase their efficacy of their ads.[98]

63. This overlap led to grave concerns about the threat to internet users' privacy. EPIC filed a complaint and urged the FTC to block the merger as the aggregation of personal data by the two companies represented a unique threat to privacy.[99]

64. Specifically, EPIC alleged that "[t]he massive quantity of user information collected by Google coupled with DoubleClick's business model of consumer profiling could enable the two companies to construct extremely intimate portraits of its users' behavior"[100] and requested that the FTC order "Google to provide meaningful notification when personal data from two distinct Google services are combined to produce a result that is linked [to] an individual user"[101] and to "[c]ondition the merger on Google and DoubleClick maintaining separate databases of user information."[102]

65. Major representatives of the technology industry expressed serious concerns about the privacy implications of the merger,[103] and the Chairman and Ranking Member of the Senate Subcommittee on Antitrust, Competition Policy and Consumer Rights together warned that "this deal raises fundamental consumer privacy concerns worthy of serious scrutiny,"[104] while the Ranking Member of the House Energy and Commerce Committee called for hearings specifically addressing the threats to consumer privacy of the merger.[105]

---

[96] Press Release, Google Inc., Google to Acquire DoubleClick (Apr. 13, 2007), http://googlepress.blogspot.com/2007/04/google-to-acquire-doubleclick_13.html.

[97] Statement of Federal Trade Commission Concerning Google/DoubleClick, F.T.C. File No. 071-0170 (2007), at 3, 6.

[98] *See* Statement of Federal Trade Commission Concerning Google/DoubleClick, F.T.C. File No. 071-0170 (2007), at 5–6.

[99] Complaint and Request for Injunction, Request for Investigation and for Other Relief, Google/DoubleClick, F.T.C. File No. 071-0170 (Apr. 20, 2007).

[100] Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Injunction and for Other Relief at ¶123, Google/DoubleClick, F.T.C. File No. 071-0170 (June 6, 2007).

[101] *Id.* ¶ 131.

[102] *Id.* ¶ 141.

[103] Press Release, Microsoft & Ask.com, Microsoft and Ask.com Call on Industry to Join Together to Evolve Privacy Protections for Consumers (July 22, 2007), https://news.microsoft.com/2007/07/22/microsoft-and-ask-com-call-on-industry-to-join-together-to-evolve-privacy-protections-for-consumers/#FcMjK16VvdL7EGYd.97.

[104] Letter from Herb Kohl, Chairman, Senate Subcomm. on Antitrust, Competition Policy and Consumer Rights & Orrin Hatch, Ranking Republican Member, Senate Subcomm. on Antitrust, Competition Policy and Consumer Rights, to Deborah Platt Majoras, Chairman, F.T.C. (Nov. 19, 2007) (available at https://epic.org/privacy/ftc/google/sen_anti_111907.pdf)

[105] *Republicans Seek Privacy Hearing on Google Deal*, Reuters (Nov. 6, 2007), http://www.reuters.com/article/us-google-congress-idUSN0639085320071106; *see also* Diane Bartz, *Lawmaker Questions Google Over Privacy Practices*, Reuters (May 21, 2008), http://www.reuters.com/article/us-toni-google-privacy-congress-

66. The FTC declined to block the merger.[106] At the time of the merger, Google and DoubleClick represented that the two companies' massive databases of user information would not be shared or merged.[107] Because of the FTC's inaction, Google has since reversed this position.[108]

I. The FTC Has Sanctioned Google for Privacy-Invasive Behavior

67. Following EPIC's complaint about Google Buzz, [109] in 2011 the FTC settled with Google a dispute regarding violations of its users' privacy in the 2010 rollout of its social media service Google Buzz.[110]

68. As EPIC alleged and the FTC subsequently agreed, Google, without consent, obtained the personal information of Gmail users, which it had promised to use only in connection with the Gmail service, to populate networks of users of Buzz.[111] Additionally, Google enrolled users in some Buzz features despite those users selecting options to "Turn off Buzz,"[112] and did not disclose key features and functions of Buzz before asking users whether they would like to enroll.[113] The FTC alleged that these actions were deceptive acts or practices.[114]

69. The consent order agreed to by Google included as one of its provisions a requirement that Google implement a comprehensive privacy program to "address privacy risks related to the development and management of new and existing products and services for consumers" and "protect the privacy and confidentiality of covered information,"[115] which was defined to include, among other characteristics, names, persistent online

---

idUSN2142539620080521 (regarding Rep. Barton's questioning Google executive Eric Schmidt personally over this issue).

[106] Statement of Federal Trade Commission Concerning Google/DoubleClick, F.T.C. File No. 071-0170 (2007), at 6–13.

[107] *Google: DoubleClick Statement Regarding Data Ownership*, Reuters (Apr. 20, 2007), https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking; Statement of Federal Trade Commission Concerning Google/DoubleClick, F.T.C. File No. 071-0170 (2007), at 12; *see also* Mc Dermott Wil & Emery, *Google-DoubleClick Merger Will Not Involve the Merger of the Two Companies' Databases*, Lexology (Feb. 28, 2008), http://www.lexology.com/library/detail.aspx?g=ca1563e6-48a2-44d1-933f-45d2e651cf83 (referring to representations made to the European Commission).

[108] Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking*, ProPublica (Oct. 21, 2016), https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking.

[109] Complaint, Request for Investigation, Injunction, and Other Relief, *In re* Google, Inc., FTC File No. 102-3136; *see also* Letter from David Vladeck, Dir., FTC Bureau of Consumer Prot., to Marc Rotenberg, Exec. Dir., Elec. Privacy Info. Ctr. (Feb. 26, 2010), https://epic.org/privacy/ftc/googlebuzz/Vladeck_Letter_GoogleBuzz.pdf.

[110] Decision and Order, Google, Inc., F.T.C. Docket No. C-4336 (Oct. 13, 2011).

[111] Complaint at ¶ 13–16, Google Inc., F.T.C. Docket No. C-4336 (Oct. 13, 2011).

[112] *Id.* ¶ 17–18.

[113] *Id.* ¶ 19.

[114] *Id.* ¶ 14, 16, 18, 19.

[115] Decision and Order at 4, Google Inc., F.T.C. Docket No. C-4336 (Oct. 13, 2011).

identifiers, physical location, and other information collected in conjunction with those characteristics.[116]

70. Google has already violated this consent order. In 2012, the FTC fined Google $22.5 million for misrepresentations to users of Apple's Safari that Google would not place "cookies", used for targeted advertising, on those users.[117]

IV. Legal Analysis

A. The FTCs Section 5 Authority

71. The FTC Act prohibits unfair and deceptive acts and practices, and empowers the Commission to enforce the Act's prohibitions.[118] These powers are described in FTC Policy Statements on Deception[119] and Unfairness.[120]

72. A trade practice is unfair if it "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."[121]

73. There are three elements to an unfairness claim. First, the injury must be "substantial."[122] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[123] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[124] Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces."[125] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[126] Finally, "the injury must be one which consumers could not reasonably have avoided."[127] This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior "unreasonably creates or takes

---

[116] *Id.* at 3.
[117] FTC, Statement of the Commission *re. United States of America v. Google Inc*. (N.D. Cal.) & In the Matter of Google Inc., FTC Docket No. C-4336 (Aug. 9, 2012); *United States v. Google Inc.*, No. CV 12–04177 SI, 2012 WL 5833994 (N.D. Cal. Nov. 16, 2012) (order approving permanent injunction and civil penalty).
[118] See 15 U.S.C. § 45 (2010).
[119] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm [hereinafter FTC Deception Policy].
[120] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [hereinafter FTC Unfairness Policy].
[121] 15 U.S.C. § 45(n); see, e.g., *Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc*., Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").
[122] FTC Unfairness Policy, *supra* note 120.
[123] *Id.*; see, e.g., *Fed. Trade Comm'n v. Information Search, Inc*., Civ. No. 1:06-cv-01099 (Mar. 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.").
[124] FTC Unfairness Policy, *supra* note 120.
[125] *Id.*
[126] *Id.*
[127] *Id.*

advantage of an obstacle to the free exercise of consumer decision making."[128] Sellers may not withhold important price or performance information from consumers, engage in coercion, or unduly influence highly susceptible classes of Consumers.[129]

74. An act or practice is deceptive if it involves a representation, omission, or practice that is likely to mislead the consumer acting reasonably under the circumstances, to the consumer's detriment."[130]

75. There are three elements to a deception claim. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[131] The relevant inquiry for this factor is not whether the act or practice actually misled the consumer, but rather whether it is likely to mislead.[132] Second, the act or practice must be considered from the perspective of a reasonable consumer.[133] "The test is whether the consumer's interpretation or reaction is reasonable."[134] The FTC will look at the totality of the act or practice and ask questions such as "how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?"[135] Finally, the representation, omission, or practice must be material.[136] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[137] Express claims will be presumed material.[138] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[139]

76. The FTC considers an omission to be material where "the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false . . . because the manufacturer intended the information or omission to have an effect."[140]

---

[128] *Id.*
[129] *Id.*
[130] FTC Deception Policy, *supra* note 119.
[131] *Id.*; see, e.g., *Fed Trade Comm'n v. Pantron I Corp*., 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron's representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).
[132] FTC Deception Policy, *supra* note 119.
[133] *Id.*
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Cliffdale Associates, Inc*., 103 F.T.C. 110, 110 (1984).

77. The Commission has previously found that a company may not alter the privacy settings of its users.[141]

B. Count I: Google's Secret, Proprietary Algorithm is an Unfair Trade Practice

78. As explained above, Google tracks its users' physical purchases with a secret and proprietary algorithm.

79. The use of a secret algorithm to match Google's behavioral user data with third-party in-store purchase information creates a substantial risk of harm. Consumer purchases can reveal medical conditions, religious beliefs, and other highly sensitive information. According to Google, it has data on 70% of all credit card and debit purchases, which represents sensitive personal information about millions of Americans.

80. The substantial risk of harm created by Google's tracking of behavioral user data to in-store purchases is not outweighed by countervailing benefits to consumers or to competition.

81. Consumers cannot easily avoid Google's tracking of their in-store purchase behavior. As described above, there appears to be no mechanism by which Google users can opt out of purchase tracking other than by disabling location tracking entirely. It is not clear to users, however, that the way to avoid tracking of *purchases* is by disabling *location* tracking.

82. Google's use of a secret algorithm to track in-store purchases is an unfair act or practice in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(n).

C. Count II: Google is Engaging in Unfair Trade Practices By Not Revealing the Identities of its Third-Party Partners

83. As explained above, Google has not revealed the identities of its third-party partners who provide credit and debit card purchase information.

84. Not revealing the source of Google's payment data creates a substantial risk of harm. If consumers do not know how Google gets its purchase data, they cannot know which cards not to use or where not to shop if they do not want their purchases tracked. The lack of disclosure thus inhibits the ability of consumers to make privacy-preserving choices or for companies to compete on privacy.

85. The substantial risk of harm created by Google's refusal to reveal the identities of its third-party partners is not outweighed by countervailing benefits to consumers or to competition. To the contrary, competition would increase if Google's arrangements with third-parties were disclosed.

86. Consumers cannot easily avoid these secretive data transfers.

[141] *In re* Facebook, Inc.; FTC File No. 092 3184, FTC.gov (Dec. 30, 2011), http://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

87. Google's refusal to reveal the identities of its third-party partners who provide it with sensitive credit card transaction data is an unfair act or practice in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(n).

D. Count III: Google's Claim that Consumers Can Opt Out of Google Tracking Their In-Store Purchases is Deceptive

88. As described and illustrated above, and contrary to Google's public representations, Google users have no clear mechanism by which they can opt out of Google tracking their real-world purchases.

89. The need for Google users to opt out of location tracking to avoid in-store purchase tracking is misleading because a reasonable consumer would have no reason to know that the latter relies on the former.

90. The misrepresentation is material because, as illustrated above, consumers find Google's in-store purchase tracking plan to be highly invasive and would avoid that tracking if they could.

91. Google's misrepresentation that users can opt out of in-store purchase tracking is a deceptive act or practice in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

V. Prayer for Investigation and Relief

92. EPIC asks the Commission to investigate Google, enjoin its unfair and deceptive business practices, and require Google to protect the privacy of its users.

93. Specifically, EPIC requests that the Commission

    a. initiate an investigation into Google's in-store sales tracking algorithm to determine whether it adequately protects the privacy of millions of American consumers;

    b. enjoin Google from misrepresenting Google users' ability to opt out of Google tracking their in-store purchases;

    c. compel Google to implement a clear and simple mechanism by which consumers can opt out of Google's tracking program;

    d. compel Google to reveal the identity of the third parties from which it collects payment transaction data;

    e. enjoin Google from implementing the Store Sales Management program with a secret, proprietary algorithm, and mandate algorithmic transparency;

    f. investigate other companies engaged in similar practices; and

    g. provide such other relief as the Commission finds necessary and appropriate.

Respectfully Submitted,

Marc Rotenberg
Marc Rotenberg,
EPIC Executive Director

James T. Graves
James T. Graves,
EPIC Law & Technology Fellow

Ellen Coogan
Stevie DeGroff
Doaa Elyounes
Brendan Heath
Cian Hanamy
Megan Iorio
Sophia McGowan
Hillary Song
EPIC IPIOP Clerks

Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)