Complaint of Disconnect, Inc.

Regarding Google’s infringement of Article 102 TFEU through bundling into the Android platform and the related exclusion of competing privacy and security technology

Case COMP/40099

June 2015

When a consumer uses his Android mobile phone to read the Financial Times’ story about the Commission’s SO against Google, he unknowingly receives 17 “network requests” from sites and services other than the FT, all attempting to open invisible connections to his device. Seven of these requests – including three from Google itself – come from problematic sites and services that invisibly track the user in order to make a comprehensive profile of his personal information as he uses applications and browses the web. This tracking not only violates personal privacy, but also leaves users vulnerable to malware and identity theft.

Disconnect Inc.’s revolutionary technologies reveal and block this problematic tracking. But Google has banned Disconnect’s blocking technology from the Google Play (mobile application) Store because it interferes with Google’s revenue stream from invisible tracking. The ban, for all intents and purposes, denies Android users the only effective protection available and makes it all but impossible for Disconnect to innovate and compete effectively.
1. **SUMMARY OF COMPLAINT**

1. Disconnect, Inc. ([https://Disconnect.me](https://Disconnect.me)), a “start-up” company based in San Francisco, California USA, develops, markets, and sells award-winning privacy and security software for mobile devices and computers. Disconnect competes in this market with Google and with a number of other software manufacturers.

2. Disconnect markets and sells its products to consumers in the EEA through its own site, through the Apple (mobile application) Store, through a distribution agreement with Blackphone and an announced agreement with Deutsche Telekom, and through various consumer “stores” of browser manufacturers. Disconnect also markets and sells some of its products through the Google Play mobile application store. Recently, Google removed Disconnect’s “malvertising” mobile application from the Play Store, leading to this Complaint.

3. When a user visits a website with his browser or opens a mobile application, third party sites and services (other than the site or service the user is trying to connect with) attempt to establish invisible, unsolicited, and frequently undisclosed “network connections” with the user’s browser or mobile device. These invisible network connections can be used to provide advertisements or content for the site or mobile application to display.

4. Frequently, however, advertising companies including Google use these invisible connections to “track” the user as he/she browses the web or opens other mobile applications, in order to collect personal information about the user, create a “profile” of the user, and make money targeting advertising to the user. Increasingly, these invisible connections (including those set up by advertising companies) are also being used even more maliciously -- by cybercriminals -- to distribute malware, steal confidential personal and business information, damage property, and engage in identity theft.

5. Authorities in the European Union have studied quite extensively the untoward intrusion on personal privacy created by advertising tracking and have enacted a set of requirements to protect internet users from the risks and intrusions of tracking, profiling and targeted advertising. These requirements are based on a regime of notice, user consent to tracking, and user choice over the extent of tracking. However, advances in tracking technology, in combination with the increasing use of mobile devices, has strained the ability of authorities to enforce compliance with these requirements.

6. Last year, following an extensive investigation, a subcommittee of the United States Senate published a bi-partisan report explaining and documenting the use of invisible network connections and tracking for cybercrime and other malicious purposes – and the associated risks to users. According to that report, “malvertising” (malicious advertising) has reached epidemic proportions putting many millions of Europeans at risk.1 Google’s sites (YouTube, for example) and advertising networks (DoubleClick, AdMob) have frequently been associated with devastating malvertising attacks.

---

7. Disconnect makes applications (including mobile applications) that protect the privacy and security of internet users by blocking invisible, unsolicited network connections between a user’s browser or mobile device and sites/services that engage in invisible tracking or are known or suspected distributors of malware.

8. Disconnect’s technology protects the user not only when he browses the web, but also when he uses other third party mobile applications. A very recent Eurecom study highlights the risks associated with invisible and largely undisclosed tracking that very large numbers of third party mobile applications distributed by the Google Play mobile application store engage in.\(^2\)

9. Google twice accepted Disconnect’s mobile malvertising application for distribution through the Play Store. Thousands of users downloaded it from the Play Store. But then Google abruptly removed it from the Play Store, claiming that Disconnect’s product violates the Google Developer Distribution because it blocks third party and other mobile applications from serving ads that Google and others sell.

10. Disconnect protested and appealed, pointing out that its app only blocks connections with sites and services that engage in mobile tracking or that are associated with malware, but to no avail. Google also threatened to terminate Disconnect’s entire Google developer account if it continued to try to publish its malvertising technology through the Play Store. So, Disconnect did not even submit its more comprehensive “all-in-one” application (that blocks the same tracking and malware sites) to Google at all, for fear of further punishment.

11. Google has a dominant position in mobile operating systems, mobile application “stores” and mobile browsers. Through control of information and interfaces, Google uses its Play Store as the only viable access point to its dominant mobile OS for third party developers.

12. There is no viable alternative mechanism for reaching the vast and overwhelming majority of mobile device users in Europe, other than through the Google Play Store. Few users are willing to complete the confusing and difficult process for installing an app on their Android devices from a site other than the Play Store – which process Google makes all the more intimidating by posting menacing warnings that are wholly unwarranted.

13. When Disconnect’s application was removed from the Play Store, it could no long be “found” by users through Google’s Play Store keyword search function, nor through Play Store search ads, nor through any of the other “finding” mechanisms available to consumers in the Play Store. Sales data for the affected applications demonstrates that Google’s conduct has foreclosed them from the market. Disconnect also lost access to interfaces and information, such that maintenance and improvement of the apps will invariably suffer.

14. Google makes mobile privacy and security software in competition with Disconnect. Google technically ties various parts of its software into its dominant mobile OS and mobile browser. Google’s software does not protect users from the risks associated with tracking. Rather, the “protections” Google offers invariably permit the company to continue to gather private information and to leave users vulnerable to malware and identity theft.

\(^2\) http://arxiv.org/pdf/1504.06093v2.pdf
15. Google also continues to publish, distribute and sell through the Play Store privacy and security software from Disconnect’s competitors. The competitors’ software does not protect users from tracking through third party mobile applications, as Disconnect’s does.

16. Google has abused its dominance in contravention of Article 102 TEUF, through various patterns of conduct, by among other actions, illegal tying, discontinuance of supply, and unjustified discrimination. Google’s conduct has retarded investment and innovation, diminished consumer choice, and facilitated the continued collection of personal information on the internet.

17. The Commission should enjoin Google from providing to Disconnect’s applications and technology anything less than treatment equal to that which Google accords to its own products that include mobile device security and privacy software and to the products of Disconnect’s mobile security and privacy software competitors – but without requiring technical tying into Google’s products.
1. Summary of Complaint ................................................................. 2

2. Disconnect Background ................................................................. 9
   2.1. Company Information ............................................................... 9
   2.2. Size of market ......................................................................... 10
   2.3. Company’s position re internet advertising ................................ 10
   2.4. Company’s technology .............................................................. 11
       2.4.1. Visualization technology .................................................... 11
       2.4.2. VPN technology ............................................................... 11
       2.4.3. Private search ................................................................. 12
       2.4.4. Private browsing .............................................................. 12
   2.5. Company privacy policy ............................................................ 14
   2.6. Accolades .............................................................................. 15
   2.7. Nexus to the EEA ..................................................................... 15

3. Tracking, Privacy and Malvertising .................................................. 17
   3.1. Data Collection ....................................................................... 17
       3.1.1. Search ad revenue ........................................................... 17
       3.1.2. Tracking ........................................................................ 17
       3.1.3. Cookies .......................................................................... 19
       3.1.4. Ad networks .................................................................... 19
       3.1.5. Other tracking technologies ............................................. 20
       3.1.6. Network requests / connections ....................................... 21
       3.1.7. Mobile app tracking ......................................................... 21
   3.2. Personal privacy ...................................................................... 22
       3.2.1. User awareness ............................................................... 23
       3.2.2. Protection regime ............................................................. 24
   3.3. User security .......................................................................... 25
       3.3.1. “Malvertising” ................................................................. 25
       3.3.2. Delivery of malware ......................................................... 26
       3.3.3. Damage from malvertising .............................................. 27
       3.3.4. Google’s malvertising ....................................................... 28
       3.3.5. Protection for users ......................................................... 28
   3.4. DNT ....................................................................................... 28

4. Google’s Market Power .................................................................. 30
   4.1. Ad tech and profiling ............................................................... 30
   4.2. The mobile platform ............................................................... 32
       4.2.1. Mobile applications .......................................................... 32
       4.2.2. Fragmentation .................................................................. 33
       4.2.3. Consolidation techniques ................................................. 34
       4.2.4. Mobile OS market power ............................................... 35
   4.3. Market power over mobile apps .............................................. 36
       4.3.1. Market power over app developers .................................. 37
       4.3.2. Monetization of market power ......................................... 38
   4.4. Market power in the Chrome Mobile Browser ......................... 39
   4.5. Abuse of dominant positions ................................................. 40

5. Google’s privacy and security software ......................................... 41
   5.1. Invisible connections ............................................................... 41
   5.2. Tying ...................................................................................... 41
6.  Google’s Exclusionary Conduct ......................................................... 51

6.1.  Browser extension ........................................................................ 51
  6.1.1.  Network connections ................................................................. 51
  6.1.2.  Block list .................................................................................. 51
  6.1.3.  Operation ................................................................................. 53
  6.1.4.  Treatment of ads .................................................................... 53
  6.1.5.  Availability .............................................................................. 53

6.2.  Mobile / malvertising app ............................................................... 53
  6.2.1.  Differences from desktop ......................................................... 54
  6.2.2.  Coverage ................................................................................. 54
  6.2.3.  VPN innovation ....................................................................... 54
  6.2.4.  Mobile block list ..................................................................... 55
  6.2.5.  Malvertising coverage ............................................................ 56
  6.2.6.  Malware list ........................................................................... 56
  6.2.7.  Product name .......................................................................... 57
  6.2.8.  Product launch ....................................................................... 57
  6.2.9.  Payment model ....................................................................... 57

6.3.  Removal by Google ....................................................................... 59
  6.3.1.  Ad blockers ............................................................................. 60
  6.3.2.  Re-launch ............................................................................... 60
  6.3.3.  Second removal ..................................................................... 61
  6.3.4.  Consumer response ................................................................. 62

6.4.  Google’s rationale ......................................................................... 64
  6.4.1.  Inconsistent with Google’s stated policy .................................... 64
  6.4.2.  Inconsistent with prior treatment and interpretation ................ 65
  6.4.3.  Discrimination: Google’s treatment of its own software .......... 66
  6.4.4.  Discrimination: Treatment of Disconnect’s competitors .......... 67

6.5.  All-in-One (AiO) application .......................................................... 69
7. Anticompetitive effects of removal .................................................. 72
   7.1. Introduction ................................................................. 72
   7.2. Loss of distribution / marketing / identification .......................... 72
   7.3. Loss of placement in search results ..................................... 73
   7.3.1. “Organic search results” .............................................. 73
   7.3.2. “Paid” search ............................................................ 74
   7.4. Loss of other placement .................................................. 75
   7.5. Loss of ability to be found ............................................... 75
   7.6. Loss of association with high quality .................................... 75
   7.7. Loss of easy downloading ................................................ 76
   7.7.1. Fragmentation Issues .................................................. 78
   7.7.2. Sideloadig procedure .................................................. 78
   7.7.3. Menu variations ......................................................... 79
   7.7.4. Menacing warnings .................................................... 81
   7.7.5. Continuing security risk ............................................... 81
   7.7.6. Additional menacing warnings ....................................... 82
   7.7.7. Locating the APK ....................................................... 83
   7.7.8. Additional warnings ................................................... 83
   7.8. Loss of GPDC functions ................................................... 83
   7.9. Loss of Upload / Install ................................................... 84
   7.10. Loss of Multiple APK Support .......................................... 85
   7.11. Loss of Capabilities Targeting ......................................... 85
   7.12. Loss of Crash Reports .................................................. 86
   7.13. Loss of Billing API ....................................................... 86
   7.15. Loss of other APIs ....................................................... 89

8. Legal arguments and remedy proposals ......................................... 90
   8.1. Markets ........................................................................... 90
   8.2. Tying / bundling ............................................................. 90
   8.3. Refusal to supply ............................................................ 91
   8.3.1. Conduct ...................................................................... 91
   8.3.2. Objectively necessary input .......................................... 92
   8.3.3. Foreclosure ................................................................. 92
   8.3.4. Consumer harm .......................................................... 92
   8.4. Denigration ...................................................................... 92
   8.5. Exceptional circumstances ................................................ 93
   8.5.1. Neighboring market ..................................................... 93
   8.5.2. Refusal Excludes Competition ....................................... 93
   8.5.3. Refusal prevents new product ........................................ 93
   8.6. Unjustified discrimination .................................................. 93
   8.7. No objective justification ................................................... 94
   8.8. No sufficient efficiencies ................................................... 95
   8.9. Remedies ........................................................................ 95
   8.9.1. Equal treatment .......................................................... 95
   8.9.2. Urgency ....................................................................... 96

Appendix A Correspondence
2. **DISCONNECT BACKGROUND**

2.1. Company Information

18. In October of 2010, Brian Kennish, then an engineer at Google, read in the business press about how the most popular apps on Facebook were transmitting users’ identifying information to dozens of advertising and internet tracking companies, without disclosure or permission. Kennish also noticed that Facebook “widgets” (e.g., the “Like” button) were transmitting the URL of the webpage the user was on, along with the user’s Facebook ID, back to the company, permitting Facebook to reconstruct the user’s browsing history.

19. Concerned that Facebook would transmit his own personal data, Kennish went home that night and wrote an “extension” for Google’s Chrome browser that disintermediated Facebook’s “Connect” functionality and blocked connections between third party sites and Facebook servers without interfering with the connection between the user and Facebook. (A “browser extension” is a small computer program that modifies, extends and enhances the functionality of the browser on which it runs.) Kennish called the product “Facebook Disconnect.” Kennish offered it free to Chrome browser users. Within two weeks, 50,000 users installed it.

20. Kennish had worked at Google for seven years, but he never worked directly with user data and did not have a good sense of what was being collected until he started reading the press articles. He quickly realized that his own employer was among the largest collectors of user data. When, in his words, he “realized what was going on,” he left Google (in November of 2010) to focus on online privacy. In December of 2010, he released the first version of “Disconnect,” a Chrome browser extension that blocked several major internet companies, including Google, from tracking users around the Web without permission. 25,000 users downloaded Disconnect in its first week.

21. On February 17, 2011, Kennish teamed with well-known privacy and consumer rights attorney Casey Oppenheim, now the company’s CEO, to officially incorporate Disconnect in the State of Delaware USA. Prior to co-founding Disconnect, Oppenheim served as General Counsel of Organic Consumers Association, helping to bring the group online and establish its prominence. Disconnect announced a round of “seed capital” in June of 2011. Investors included venture capital firms Charles River Ventures and Highland Capital Partners. The company subsequently announced its “A Round” of financing, led by FirstMark Capital in June of 2013.

---

22. In April 2013, Disconnect was certified as a “B Corporation.” B Corporations are new types of corporate entities, “benefit corporations,” recognized by legislation in many of the states of the U.S. They operate in a similar manner to traditional corporations, but with “higher standards of corporate purpose, accountability, and transparency.” To attain the status of B Corporation, a company must submit to evaluation and certification by B Lab, a U.S. nonprofit organization. As a B Corporation, Disconnect is able to focus on consumer advocacy and education, and collaboration with non-profit consumer protection groups, along with creating for-profit products.

23. Over the years, Disconnect’s product offering has grown from a single browser extension to a robust suite of desktop and mobile products -- a full-fledged platform, in fact -- focused on personal privacy and user security on the internet. Today, over ten million people use Disconnect software. Disconnect competes in the development, distribution and sale of mobile privacy and security client software against Google (as explained below), Ghostery (as explained below), and a number of other companies, including AnchorFree, AVG, F-Secure, Symantec, Lookout and Albine.

2.2. Size of market

24. Gartner, the technology research group, estimates that the global cybersecurity market will grow from $67 billion in 2013 to $93 billion in 2017. Sales of mobile device security client software alone are expected to reach $3.4 billion by 2018.

2.3. Company’s position re internet advertising

25. Disconnect is not opposed to internet advertising -- far from it. The company recognizes the important role of advertising in the provision of information and services on the internet. Rather, the purpose of the company is to enable users to control their online data, the first step of which is to help users understand data collection and stop the free flow of personal information to undisclosed third-party websites and services.

---

10 http://www.bcorporation.net/community/disconnect-inc
11 See http://www.bcorporation.net/what-are-b-corps/the-non-profit-behind-b-corps
12 http://techcrunch.com/2013/06/17/disconnect-an-ex-googlers-social-enterpriseprivacy-startup-raises-3-5m-extends-to-more-browsers/
13 http://techcrunch.com/2012/03/22/disconnect-me-raise/
14 https://disconnect.me/
20 http://techcrunch.com/2012/03/22/disconnect-me-raise/
26. In the company’s view, all online data collection should be consensual. “I would like to see Google only collect data that I explicitly allow them to collect,” Kennish has explained.\(^{21}\) Hence, where appropriate, it is Disconnect’s general policy not to stop the collection of tracking information by any company that commits to honor users’ Do Not Track (DNT) designations and agrees to comply with the DNT rules and policies established by the Electronic Frontier Foundation (EFF) or other comparable organizations.\(^{22}\)

2.4. Company’s technology

27. Disconnect has developed and released four types of functionality: visualization of undisclosed web tracking and privacy policies; virtual private networking (VPN) technology; private search; and private browsing. From the language of Google’s written communications with Disconnect described below, Google’s actions against Disconnect focus on Disconnect’s “private browsing” functionality. However, the four types of functionality have appeared in various combinations in various Disconnect products released over the last several years, so the “private browsing” functionality is not confined to a single Disconnect product.

2.4.1. Visualization technology

28. Disconnect first launched its “visualization” functionality as an extension for Google’s Chrome browser in April of 2012. This technology displays a map for the user of all tracking requests (including social networking, analytics and advertising) from any webpage visited by the user.\(^{23}\) In June of 2014, Disconnect released a different type of visualization tool – a browser extension that analyzes and explains the privacy policies and data practices of websites through an easy to understand set of visual clues (icons).\(^{24}\)

2.4.2. VPN technology

29. In June of 2014, Disconnect also released a product, “Secure Wireless,” that included, among other functionality, VPN technology intended to protect all network connections in order to prevent eavesdropping over Wi-Fi and cellular networks, the theft of user passwords, credit card information, etc. The product is currently available as an Android app through Google’s Play Store and comes pre-installed on Blackphone devices (described below).\(^{25}\) The VPN technology encrypts all of the user’s internet connections. Some of Disconnect’s VPN implementations also provide “location control” by changing the user’s IP address and masking the locations of the company’s VPN servers, so as to defeat internet censorship and permit user access to blocked websites.

---

22. [https://disconnect.me/help#does-disconnect-block-all-ads-is-it-an-adblocker](https://disconnect.me/help#does-disconnect-block-all-ads-is-it-an-adblocker)
2.4.3. **Private search**

30. As explained below, most search engines collect and store records of search queries in order to customize user search results, select ads for presentation to the user, and create user profiles linked (with the aid of IP addresses) to the user’s personal identity.²⁶ Google also provides search query data to its advertisers.²⁷

31. In October of 2013, Disconnect first launched a browser extension with “private” (or anonymous) searching functionality, designed to allow users to keep their searches private while continuing to use the most popular search engines. This product encrypts user search queries and routes them through the company’s servers so that search providers cannot associate the queries with particular users or their computers. Nor, as a result, can search engines pass the user’s search terms to sites (including advertising sites) the user visits from the search results page.²⁸ Disconnect subsequently released this functionality through a webpage, as an Android app available through the Google Play Store, and pre-installed as the default search provider on Blackphone devices.²⁹

2.4.4. **Private browsing**

32. Permitting users to browse the web without being non-consensually and invisibly tracked, and therefore exposed to attendant security and privacy risks, has been a key goal of the company since its inception. As noted above, Disconnect first launched a browser extension that blocked “third party tracking” (explained below) from Google, Facebook, Twitter, and several other companies in 2010.³⁰ A more advanced version of this browser extension product, released in April of 2013, expands blocking to more than 2000 invisible tracking sites/services as well as “social widgets” (e.g., Like, Tweet and +1 buttons), and also incorporates web tracking visualization functionality.³¹

---

²⁹ [http://www.reuters.com/article/2014/03/24/ca-disconnect-idUSnBw245347a+100+BSW20140324](http://www.reuters.com/article/2014/03/24/ca-disconnect-idUSnBw245347a+100+BSW20140324)
33. Disconnect continued to enhance its private browsing technology and in the late summer of 2014 quietly launched an even more robust version of its private browsing functionality, this time as an application for the mobile platform (both Google’s Android and Apple’s iOS). The product blocks invisible connections between the user’s device and known or suspected malware sites, in addition to potentially malicious tracking sites and services – thousands of sites in all – affording the user protection both on mobile browsers and within other mobile applications. At launch, the product was called “Disconnect Mobile,” but the company changed its name to “Disconnect Malvertising” (the name by which it is generally referred to in this Complaint) to avoid confusion with other Disconnect products.

34. Google initially issued Disconnect the appropriate authorization codes for the product and permitted the app to be sold from the Google Play Store, but then abruptly (and without warning) removed the app from the Play Store. Following an enormous outcry in the press, Google briefly accepted the app in the Play Store, but then banned it again. Because Google’s actions toward the malvertising product form the crux of this Complaint, the development of the product, its functionality, and Google’s conduct toward it are described in greater detail below.

\[32 \text{ See } \text{https://blog.disconnect.me/blog/google-just-banned-our-new-android-app-before-it-even-launched-another-example-of-why-privacy-friendly-alternatives-for-android-app-distribution-are-critically-important} \]

\[33 \text{ See } \text{https://blog.disconnect.me/blog/update-android-app-is-still-banned-from-play-and-google-wont-talk-about-it} \]
35. In November of 2014, Disconnect released an “all-in-one” application (“AiO app”) that combines the key types of functionality from the individual Disconnect products into a single integrated application. The product works seamlessly across user devices -- mobile (the Android and iOS platforms) as well as desktop (for the Windows and Mac platforms). The sites and services blocked by the “all-in-one” (AiO) application are virtually identical to those blocked by Disconnect’s malvertising application, previously banned by Google from the Play Store.

36. Even beyond privacy and security, Disconnect’s products help users as they browse the web because the company’s filtering is optimized for speed to accelerate web browsing; using the Disconnect applications, the webpages that users visit load much faster and use less bandwidth than they would without the Disconnect’s technology.

2.5. Company privacy policy

37. Disconnect operates under a very strict and very clear privacy policy. Its products do not collect any data that can identify a particular person. Its website does not collect IP addresses or geolocation information. And neither its products nor its site collect information about users’ online activities over time and across third party websites or online services. Disconnect’s products are “open source” so that anyone can inspect the code to see how it works and how it handles user information. In fact, other developers can inspect the code and even “fork” it – use it for their own purposes without permission.

38. Disconnect makes money by selling its products to users, not from selling user information to advertisers or data brokers. The company has a two-part pricing model. For browser extensions, users can “pay-what-they-want” and earmark a portion of their payment for privacy-protecting non-profits. For mobile software applications, Disconnect offer a “Basic” version free and “Premium” version with greater functionality for monthly or yearly payments.

36 http://techcrunch.com/2013/04/17/disconnect-2-brings-more-privacy-to-your-browser-lets-you-block-2k-sites-from-tracking-your-activity-online/
37 https://disconnect.me/privacy
38 https://disconnect.me/help#how-do-i-know-that-disconnect-itself-isnt-logging-and-selling-my-data
41 http://techcrunch.com/2013/04/17/disconnect-2-brings-more-privacy-to-your-browser-lets-you-block-2k-sites-from-tracking-your-activity-online/
42 https://disconnect.me/help#how-do-you-make-money-
2.6. Accolades

39. Disconnect’s products have consistently received top industry awards and honors. In 2013, Popular Science named Disconnect’s private browsing extension one of the top 100 innovations for 2013. DataWeek recognized Disconnect with a “Top Innovator” award the same year. And Launch Media named Disconnect the conference winner for “Best Technology” among existing companies with new products. In 2014, Lifehacker Pack named Disconnect’s browser extension for Firefox an “essential application” in the security category.

40. In 2015, PC Magazine named Disconnect’s product one of the best Google Chrome extensions. More recently, Disconnect won the 2015 Interactive Innovation Award for “Privacy and Security” at the prestigious South by Southwest Conference. The award is given for “2014’s most progressive accomplishment in the way we go about securing our data and ensuring our privacy.”

2.7. Nexus to the EEA

41. For the last several years, Disconnect has distributed and sold its products, and otherwise made them available, to consumers in the various countries of the EEA, and consumers within the EEA have downloaded and purchased those products. Disconnect has distributed its products to EEA consumers through the Google Play Store, the Apple Store, the Google Chrome Store, and its own site (Disconnect.me). For example, below are some of the statistics that Google has provided to Disconnect on the Google Play Developer Console evidencing the number of “installs” through the Google Play Store of Disconnect’s private searching application for the Android platform as of January 4, 2015:

http://www.prweb.com/releases/2013/11/prweb11325674.htm
http://dataweek.co/2013/?page_id=54
http://dataweek.co/2013/?page_id=54
http://www.pcmag.com/article2/0,2817,2423665,00.asp
http://sxsw.com/interactive/awards/interactive-awards
http://sxsw.com/interactive/awards/categories
https://play.google.com/store/apps/details?id=me.disconnect.search
42. Disconnect’s mobile malvertising app that was removed from the Play Store by Google remains available for download and purchase by consumers within the EEA from the Disconnect site. Disconnect’s private searching app for the Android platform remains available for download by EEA users through the Google Play Store, as does Disconnect’s Secure Wireless mobile application. Disconnect’s all-in-one (AiO) application (including the malvertising functionality) is available to EEA consumers through the Disconnect site, and through the Apple Store.

43. Deutsche Telekom has announced a partnership with Disconnect pursuant to which DT will distribute the new Disconnect software as part of a special promotion to encourage DT users to protect themselves online. And, SGP Technologies of Geneva, Switzerland (with major operations in Madrid and offices throughout Europe), pre-installs the Disconnect application on all of its Blackphone privacy-oriented smartphone devices.
3. TRACKING, PRIVACY AND MALVERTISING

3.1. Data Collection

44. In order to understand the significance of Google’s actions against Disconnect’s malvertising product, it is helpful to understand at a conceptual level the basic problems that Disconnect is trying to address – threats to the internet privacy and security of users. The quest for revenue from advertising is driving the collection of user data by web companies. Web companies collect user data from the internet in two important ways – by collecting records of search queries and by tracking users as they browse the web and use applications.

45. User data has become the fundamental currency and revenue generator of the new internet economy, a point made by Commissioner Vestager at her confirmation hearings. Commissioner Vestager views data collection as an issue of competition policy as well as personal privacy. In this Complaint we add one additional concern about data collection to those already on Commissioner Vestager’s mind: Data collection through internet tracking does not just threaten personal privacy. It also leaves users vulnerable to malware and other cybercrime, including identity theft. All of these concerns can be addressed, at least to a substantial extent, merely by enjoining Google’s abuse of its dominant position, as described in this Complaint.

3.1.1. Search ad revenue

46. Most search engines collect and store records of search queries. Search engines use the search terms (and the user’s history of searches) to select ads to present to the user along with the search results. Ads that reflect the user’s interests most closely command the highest prices because of their high response rates. So search ads – selected to correspond to what the user is already looking for – have long been a lucrative source of revenue.

3.1.2. Tracking

47. Advertisers also try to engage users more generally, as they browse the web and use applications. Originally, online advertisers bought ads based on proximity to content related to the subject matter of the ads. But, over time, advertisers began paying for ads only if a user clicked on them. Ads that are specifically tailored and directed to particular user’s tastes and interests produce higher response rates than those that are not tailored. Advertisers,
therefore, will pay a huge premium – 60 to 200 percent for ads that are targeted in this manner.\footnote{Beales, Howard and Eisenach, Jeffrey A., An Empirical Analysis of the Value of Information Sharing in the Market for Online Content (January 2014) (available at SSRN: http://ssrn.com/abstract=2421405 or \url{http://dx.doi.org/10.2139/ssrn.2421405} )}

48. In order make the most money from selling online advertising, then, companies have to accumulate enough information about a user’s tastes, interests, and behavior to know what kinds of ads to direct to that user. The best source of such information is a user’s web browsing history.\footnote{http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/} So, companies began to track users as they clicked from site to site and from page to page within a site on the web. The accumulated information is used to create dossiers – profiles – of each user.\footnote{See Article 29 Working Party, Opinion 2/2010 on online behavioural advertising (June 22, 2010) at 4. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (cited as “Opinion 2/2010” and similar citation forms for other WP opinions) ; http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/} Records of search queries are also included in user profiles so that ads can be targeted even when the user is not on the search engine’s site.\footnote{See “Online Advertising and Hidden Hazards to Consumer Security and Data Privacy,” Permanent Subcommittee on Investigations, United States Senate, May 13, 2014 (hereinafter, “Senate Report”) at 14; Opinion 2/2010 at 4. See, e.g., Opinion 2/2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf}

49. Online advertising networks use this information about a user’s browsing history to identify the user’s interests, demographic information, etc. so that the ad network can decide which advertisement would be best (i.e., most likely to produce a click) to serve to that particular user.\footnote{http://www.nytimes.com/2008/03/10/technology/10privacy.html?ref=slogin} This technique is called “behavioural” or “targeted” advertising, a subject that European Union authorities have studied extensively.\footnote{See, e.g., Opinion 2/2010.}

50. Opinion 2/2010 (“Online Behavioural Advertising”) of the Article 29 “Working Party on the Protection of Individuals with regard to the Processing of Personal Data,”\footnote{http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf} contains an excellent description of how online companies track and transmit user information. However, online advertising distribution systems have become far more complex since the publication of Opinion 2/2010 in June of 2010. This new complexity is particularly relevant to the proliferation of sources of user tracking and the attendant risks of malware and identity theft.

51. A somewhat more up-to-date description of how online companies track and transmit user information can be found in a report published last year, after an extensive investigation, by a permanent subcommittee of the Unites States Senate. The report is bi-partisan, meaning that the information, conclusions and recommendations in the text of the report embody the views of the representatives of both political parties. The Report can be downloaded from the Subcommittee’s hearing site.\footnote{http://www.hsgac.senate.gov/hearings/online-advertising-and-hidden-hazards-to-consumer-security-and-data-privacy} For purposes of completeness, we review a portion of the material in Opinion 2/2010 and in the Senate Report below.
3.1.3. Cookies

52. Historically, “cookies” have been the primary mechanisms by which companies track and transmit data about internet users. When a user visits a webpage, the user’s browser sends a request to the webpage’s server to load the requested page. The webpage’s server usually responds with the requested content and a “cookie.” Cookies are small text files placed on the user’s hard drive or browser that identify the user’s computer and in the aggregate provide a store of information about a user’s interactions with websites.73

53. A cookie placed by the site actually visited is called a “first party cookie.” This type of cookie is frequently used to help the site function, by, for example, counting the number of unique visitors or allowing the site to “remember” what a user put into an online shopping cart.74

54. Usually, the webpage’s server also instructs the user’s browser to contact one or more third party sites that respond with requested content (advertisements for example) as well as cookies of their own. These are called “third party cookies.”75 Online advertisements from third party sites sometimes deliver whole programs, not just cookie files, to a user, even if the advertisement appears to be just an image.76

55. The material requested from a third party by the webpage’s server need not even be as large and distinct as an advertisement. Indeed, it might be almost invisible – often a single pixel. But this still entitles the third party to place its own cookie on the user’s browser.77 Third party cookies are generally used for tracking and monetization.78

3.1.4. Ad networks

56. Third party cookies come from a large number of sources. For example, a webpage’s server has to contact an ad network every time it needs an ad. An ad network is an intermediary between host websites and advertisers – usually an ad platform operated by a large tech company (like Google) – that in effect manages ad space on websites. Using data collected from cookies and other sources, the ad network might decide which advertisement should be sent to a user, but it does not itself supply any ads. Rather, using “ad tags,” it directs the user’s browser to contact a server designated by the advertiser. That server actually supplies the ad to the user’s browser.79

57. Although the ad network does not actually supply the ad that is posted, each call for an advertisement to the ad network allows the ad network to place a third party cookie in the user’s browser.80 In addition, tracking companies (entities in the business of gathering and selling data about people) often pay websites to distribute their cookie (or other tracking) files

74 Senate Report at pp. 10 – 14.
76 Senate Report at p. 13.
77 Senate Report at pp. 10 – 14.
78 http://www.allaboutcookies.org/privacy-concerns/
80 Senate Report at p. 12.
by contracting with the website to place a single pixel on the website. Some tracking companies hide their own tracking files in other tracking files, ads, or software provided to the websites, so that websites do not always know when they are distributing tracking files to users.

58. Almost every website calls some third parties that operate cookies on the site. So pervasive and intrusive is online user surveillance and tracking that a study several years ago by the Wall Street Journal revealed that the 50 top websites in the U.S. on average installed 64 pieces of tracking technology onto the computers of visitors. These “trackers” were invisible to the user and were usually installed in the U.S. without warning or consent. Of course, European Union rules require disclosure of and user consent to the use of cookies by websites. But, as we describe below, advances in tracking technology and the proliferation of “malvertising” render these rules increasingly problematic with respect to the protection of users.

59. Once a cookie is placed, it can be “read” the next time the user clicks on a site affiliated with (or part of) the same network as the tracking company or network that first placed the cookie. The network or tracking company can take note of the sites the user has visited (and other things such as what the user has purchased) and over time compile a very complete profile of the user.

60. In response to criticism, ad networks and tracking companies invariably claim that cookies do not pick up the personal identities of the individuals they are tracking, but only identifiers of the users’ computers, like IP addresses. This is technically correct, but it is easy for companies that collect online information to match the computer identifiers with other available information so that the personal identity of each user can be confirmed and tracked. Indeed, as a member of the U.S. Federal Trade Commission observed last year, the “whole point” of data brokers, tracking companies and internet companies creating user profiles is to link them to personal identities that include not only names but also medical histories, medications, political affiliations, religion, etc.

3.1.5. Other tracking technologies

61. Although many lay people think of “cookies” and “trackers” as synonymous terms, they are not. Cookies, in fact, are a relatively primitive form of tracking. “Flash cookies,” “beacons” (including “pixel tags” and “web bugs”), “history sniffing,” and “fingerprinting” are all more sophisticated and nefarious methods to track users, create profiles and attach personal identities to them. Frequently, these techniques cannot be disabled through the traditional privacy settings of a

---

81 Senate Report at p. 12.
82 http://www.wsj.com/articles/SB10001424052748703940904575395073512989404
83 Senate Report at p. 10 – 11.
84 http://www.wsj.com/articles/SB10001424052748703940904575395073512989404
85 http://www.wsj.com/articles/SB10001424052748703940904575395073512989404
87 http://www.networkworld.com/article/2168144/malware-cybercrime/can-your-ip-address-give-away-your-identity-to-hackers—stalkers-and-cybercrooks-.html
web browser. And, they will continue to work even if cookies are deleted. Some of these record what is being typed by a user on a webpage or where the mouse is moving. Others can be used to re-install regular cookies after a user has deleted them.

62. The use of cookies on mobile devices and inside mobile apps is not as prevalent as it is on the desktop computer. Data brokers and other companies interested in identifying users and creating profiles use “fingerprinting” and other forms of device identification for tracking on mobile devices. Fingerprinting permits a website, third party, or even the publisher of an API to clandestinely ascertain various identifying characteristics of a user’s device, including settings, screen size, installed software and updates, etc. Using fingerprinting, marketing companies can identify 98% of internet users, monitor their online activities, and target ads to them.

3.1.6. Network requests / connections

63. All of these tracking and personal identification techniques use (and operate through) “network requests” between the user’s device, browser or other application and a webserver or service that is attempting to record information from the user’s device. They all operate invisibly, and without warning to or consent by the user, except to the extent required by European Union rules (and assuming compliance).

3.1.7. Mobile app tracking

64. As we explain in greater detail below, the principal issue in this Complaint arises from invisible, nonconsensual tracking by mobile applications downloaded onto users’ smartphones. This is a subject of great concern within the European Union, which the Article 29 Working Party addressed a couple of years ago. Google removed Disconnect’s product from the Play (mobile application) Store because it blocks such tracking.

65. A very recent study published by security researchers at Eurecom analyzed invisible tracking by mobile applications available on the Google Play Store (hereinafter “Eurecom study”). The study’s findings strongly support both the Working Party’s concerns about mobile app tracking and Disconnect’s approach to the problem. The Eurecom study has been favorably reviewed in a leading U.S. technology journal.

66. The Eurecom study found that once a user installs a mobile application for Google’s Android operating system from Google’s Play Store, “the user has no visibility into who the application is

---

actually communicating with.” Some applications invisibly connect to almost 2000 different URLs -- in addition to the one the user is actually trying to connect to. “[U]sers are rarely aware of the actual entities that are tracking them,” the study states.95

67. The study revealed that over 66% of the free Android applications analyzed connect invisibly with URLs that serve ads. Some of these, according to the study, collect detailed device identifying information96 – which, of course, can be used for fingerprinting and related tracking. The “average number” of ad-serving URLs that connect with Play Store applications is “about 40.” “The three most prominent” domains corresponding to these URLs “are all part of Google.”97 The domain the apps most frequently connected with (invisibly) in the study was doubleclick.net, part of Google. As the study states, DoubleClick is “an advertising platform that tracks end-users, and also serves up advertisements.”98

68. In addition, more than 25% of the apps invisibly connect to tracking services that do not serve ads, but still “construct profiles.” The top 16% of these apps “connect to 100 or more trackers.” Google has awarded its “Top Developer Badge” to 4 of the 10 apps that invisibly connect to the largest number of tracker URLs.99 Finally, a smaller percentage of the apps connect to URLs corresponding with “suspicious” domains – those associated with malware or illicit content.100

69. The study concludes, “[t]he results presented thus far clearly indicate that applications on the Google Play Store often connect to destinations that are not essential for the operation of the app itself. Furthermore, much of this communication is completely hidden from users.”101

70. Online advertising has become a key component of the global economy.102 Online advertising is based on tracking, so user tracking, profile creation, and personal identification have become more and more pervasive.103 The proliferation of tracking and other user identification techniques has produced two significant issues for internet users and government officials: personal privacy and user security.

3.2. Personal privacy

71. Governmental authorities in the European Union have long recognized the challenges to personal privacy posed by user tracking and behavioural advertising on the internet and have led the world in protecting user privacy. In 2002, the European Parliament and Council enacted its famous e-Privacy Directive (2002/58/EC), which it amended in November of 2009 (2009/136/EC).104 Throughout the years, the objectives and requirements of the e-Privacy

---

95 http://arxiv.org/pdf/1504.06093v2.pdf (at 1, 2).
103 http://www.wsj.com/articles/SB10001424052748703940904575395073512989404
Directive, as amended, have been explained and applied in various opinions of the “Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data,” which we cite throughout this Complaint. Enforcement, of course, is left to the Member States.

72. In Opinion 16/2011, the Article 29 Working Party noted “a growing concern amongst citizens, politicians, data protection authorities, consumer organizations, and policy makers that the technical possibilities to track individual internet behaviour over time, across different websites, were rapidly increasing.” The Working Party also noted that “the possibilities offered to citizens to protect their private life and their personal data against this type of tracking were not keeping pace with this growth.”

3.2.1. User awareness

73. User awareness: According to the Article 29 Working Party, the average European internet user is not aware that his online behaviour is being tracked, or for what purpose. Commissioner Vestager made the same point in a more recent interview. Surveys show that notwithstanding the lack of a detailed knowledge of tracking, 72% of Europeans worry that they give away too much personal data, and 70% are concerned that their personal data is being misused.

74. Perhaps some users are comfortable with the notion that they can be tracked around the web anonymously for the purpose of showing them targeted advertisements. But very few users (or government officials, for that matter) understand that complete profiles, including all aspects of their lives, their names, and other indicators of their personal identities, have been prepared from tracking data. In other words, users are tracked by name. Few users would be comfortable with that, if they had knowledge of it.

75. Nor is this information used only for targeting advertising, at least in the U.S. Among other things, it is used to target financially vulnerable individuals for exploitation by unscrupulous loan companies. And it is sold to employers for evaluating job applicants, without disclosure to the individuals. In fact, although some large websites keep the data they collect for their own purposes (including advertising), the data invisibly collected by tracking companies in the U.S. is widely available for sale for unknown ultimate uses. Most users would be shocked to learn these facts.

---

3.2.2. Protection regime

76. European policy makers, according to the Article 29 Working Party, have “strong doubts” about relying on the online advertising industry “to increase public awareness and user choice with regard to online behavioural advertising.” So, European governmental authorities enacted (through Article 5(3) of the e-Privacy Directive, as amended, as well as Working Party Opinions) a set of requirements for website operators (and others) to protect internet users from the risks and intrusions of tracking.

77. The requirements are based on a regime of notice, user consent to tracking, and user choice over the extent of tracking -- specifically (among other possible components),

   a. “Immediately visible” notice that the website uses tracking mechanisms;

   b. Notice that the user consents to the tracking by using the site; and

   c. A mechanism by which the user can choose to accept all or some or decline cookies.

78. The requirements are not restricted to HTTP cookies, but also apply to “similar tracking technologies.” In Opinion 9/2014, the Article 29 Working Party concluded that the requirements of Article 5(3) of the e-Privacy Directive, as amended, applied to device fingerprinting.

79. However, the Article 29 Working Party has observed over the years that advances in tracking technology (and in combination with the increasing use of mobile access to the internet) have strained the abilities of authorities to enforce compliance with the Article 5(3) requirements – particularly the notion that users be given a mechanism to accept all, some or decline all cookies. In Opinion 2/2010, for example, the Working Party noted that “flash cookies,” cannot be deleted through the traditional privacy settings of a web browser. And in Opinion 9/2014, the Working Party described how third parties that provide advertising services can use fingerprinting to track users and create profiles “in a covert manner and without the knowledge of the user,” even if the user declines cookies. Moreover, while a user can identify and remove

---

a conventional “cookie” text file, the user cannot modify or remove the elements employed by third parties for fingerprinting.119

80. On February 27, 2013, after extensive study, the Article 29 Working Party published an opinion directed to the collection and processing of personal data by smart phone applications.120 The Working Party noted that third parties can get access to “unique identifiers” for smart devices, many of which “cannot be deleted or changed by users,” that permit users to be “singled out” and served with targeted services, including advertisements.121 Many free mobile apps, the Working Party observed, are paid for by advertising enabled by device-identifying tracking facilities delivered through icons on the mobile desktop.122

81. The Working Party therefore concluded that mobile operating system manufacturers must “[p]rovide user-friendly and effective means to avoid being tracked by advertisers and any other third party” and “offer users sufficient control to exercise valid consent over the data processed by apps.”123

82. As we explain below, the Disconnect technology that Google has banned from its Play (mobile application) Store enables users to exercise the option to decline tracking on mobile devices, as contemplated by Article 5(3). The various user privacy products and features that Google has incorporated technically into its own dominant platforms do not. Nor do the mobile applications, made by Disconnect’s competitors, which Google favors in a discriminatory manner by continuing to include them in the Play Store.

3.3. User security

83. The risk to users from tracking and the collection of personal information goes far beyond merely the loss of personal privacy. The same technology that permits advertising and analytics tracking -- invisible, unsolicited “network connections” between the user’s browser or mobile device and sites or services other than the one the user is trying to connect to -- exposes users (and their employers) to enormous costs associated with damaging computer viruses, identity theft and misappropriation of confidential information.

3.3.1. “Malvertising”

84. Many users are familiar with the concept of “malware” – malicious software. They understand, for example, that they can infect and damage their computers and expose themselves to risk of theft of confidential information from their computers by clicking on a site that distributes malware.

121 Opinion 2/2013 at 12.
123 Opinion 2/2013 at 29.
85. But few users understand that cybercriminals distribute malware to unknowing users through corrupted advertisements and surreptitiously mine advertising trackers for users’ personal information. This group of user security problems associated with tracking has not been studied in Europe nearly as extensively as privacy violations from tracking.

86. The subcommittee of the United States Senate referenced above has studied this problem. See Senate Report. In fact, in the United States, there is a term for this problem – “malvertising.” But neither the concept nor the term are widely known in Europe, despite the fact that some of the most infamous malvertising attacks involved large numbers of European users.\textsuperscript{124}

87. As the Senate Report explains, the sale and delivery of online advertising has become increasingly complex – first with the advent of ad networks, then ad exchanges, then supply- and demand-side platforms.\textsuperscript{125} As a result, there are usually five or six intermediary companies between the website the user is visiting and the advertiser whose ad is ultimately served to the user.\textsuperscript{126} The complexity of the system gives cybercriminals many opportunities to insinuate malware which they accomplish in a number of ways.

88. Most commonly, the cybercriminal simply goes from ad network to ad network, paying to run what are actually malicious ad campaigns until they are detected and shut down. More sophisticated criminals impersonate legitimate advertisers or ad agencies, sometimes by using stolen credentials, to gain access to the website being visited. Increasingly, criminals are hacking servers involved in the ad selection and delivery process, and thereby compromising existing ads or directly inserting malicious ads.\textsuperscript{127}

3.3.2. Delivery of malware

89. When an ad opens in a user’s browser (or in a third party mobile app), that action usually opens an invisible connection to a third party server/site/service that the user has not requested, through which user information (e.g., IP address, digital fingerprint, URL of visited website, etc.) is passed. The user information passed through the invisible network connection can be used to identify and track the user for the purpose of targeting advertising. As explained above, the third party service usually inserts one or more tracking connections into the user’s browser or mobile app.

90. But if the third party server is controlled (either through ownership or hacking) by a purveyor of malware, that entity receives the user’s confidential information through the invisible network connection. The third party server can also place malware (and additional cookies for malicious purposes) into the user’s browser or mobile app.

\textsuperscript{124} See, e.g., Senate Report at p. 28.
\textsuperscript{125} See Senate Report pp. 16 – 23.
\textsuperscript{126} Senate Report at p. 14.
91. So, a user’s computer or device can become infected with malware from a malicious ad merely by loading the website or using the mobile app on which the ad appears because that action opens the invisible network connection. The user need not click on the ad or interact with it in any other way. In fact, the malicious ad might not even become visible to the user. Rather, when the website’s server or mobile app opens a connection to a third party’s server, the malware purveyor may simply deliver malware directly to the user’s browser or mobile app instead of delivering the advertisement’s image.  

92. The owners of the website being visited or the mobile app being used by the user likely would not even know their site/app was displaying tainted ads or facilitating connections that harm the user. Indeed, the complexity of the ad delivery system is such that it is frequently impossible to identify the original source of a malicious ad, even after the malvertising incident has become publicly known.  

93. The estimated number of malvertising incidents has soared in recent years. In 2013, there were more than 200,000 malvertising incidents generating over 12.4 billion malicious ad impressions. A study by a well-known Silicon Valley company found that internet users are 182 times more likely to get a computer virus from an online ad than from surfing the web for pornography.  

94. Consumers routinely and unknowingly encounter malvertising on popular and reputable mainstream sites. A recent study has shown that more than half of internet website publishers have suffered a malware attack through online advertising. Some of the largest ad networks – including Google’s ad network – have delivered malware to consumers via advertisements on the sites of unsuspecting publishers.  

3.3.3. Damage from malvertising  

95. Cybercriminals distribute malware through online advertising in order to send spam, commit fraud, steal sensitive information, and commit vandalism and sabotage against user devices and network systems (including banking and government networks). They also use malvertising to monitor internet activity and record user keystrokes, subjecting users to the risk of identity theft and financial ruin. If a user has work files and accounts on his personal device, the cybercriminal can get access to and control over the employer’s information, including login credentials and company data. The Senate Report documented cases in which malvertising infected users with viruses intended to break into online bank accounts, steal personal data, and extort money from users, as well as malware that seized control of users’ computers.
96. Cookies and other means of tracking can also be used more directly for malicious purposes. For example, cybercriminals can include cookies in malware they distribute. The cookies identify infected computers to the cybercriminal and thereby facilitate the cybercriminal’s ability to seize control over the infected computers.

97. Even conventional advertising trackers can be attacked, “hijacked” and scanned by a criminal to gain access to the user’s confidential login information, again facilitating fraud, identity theft, data breaches involving employer information, etc. And once advertising trackers are compromised, the “normal” data collected by the trackers for online advertising permits cybercriminals to identify and target their activities to the consumers who are most vulnerable and to take specific steps to avoid detection.

3.3.4. Google’s malvertising

98. Google’s sites, services, and ad network are frequently linked to malvertising incidents that have caused widespread consumer injury, as we describe in considerable detail below.

3.3.5. Protection for users

99. As the Article 29 Working Party has recognized, advances in tracking technology, coupled with the widespread use of mobile devices to access the internet, increasingly constrains the ability of authorities to protect personal privacy through a disclosure and consent regime. The prevalence of malvertising compounds the problem. Users are not warned about the heightened risks of malware, identity theft, and other forms of cybercrime when they agree to advertising tracking on a site or mobile app. And while the EU’s consent requirements certainly contemplate giving users the ability to decline some or all tracking (which, given the associated malvertising risks, most if not all users would want), this component of “consent” has not actually been implemented widely by websites, developers or OS providers in the EEA with respect to mobile apps.

100. Infringements of personal privacy through the creation of user profiles and risks to user security from malvertising both stem from invisible network connections. So, one straightforward approach for dealing with both issues is to provide users with a mechanism to block invisible network connections. Disconnect’s technology does just that.

3.4. DNT

101. More generally, to address tracking where users engage the internet through browsers (as on the desktop), privacy advocates have proposed a Do Not Track (“DNT”) system. Under a “Do Not Track” (DNT) system, websites, advertising networks, advertisers, data brokers, etc. honor a user’s request, communicated through his browser setting, not to be tracked while browsing the web.

135 http://www.bitdefender.com/support/cookie-threats-1.html

136 Senate Report at p. 25.

102. The Article 29 Working Party has repeatedly recognized the promise of a DNT system. See, e.g., Opinion 9/2014 at 7; Opinion 16/2011 at 10. In fact, the Chairman of the Article 29 Working Party has said, “[a] global do-not-track mechanism could be a very efficient way to deal with user consent for the tracking of web surfing behavior.” The former Digital Agenda Commissioner, Neelie Kroes, has also expressed interest in a DNT system.

103. A widely respected public interest group in the U.S. (Electronic Frontier Foundation) has proposed a well-considered DNT policy, in the form of a text file that domains can post verbatim so that other software can tell that the posting domains will respect a meaningful version of DNT. The expertise of the EFF on personal data collection techniques has been cited by the EU’s Article 29 Data Protection Working Party.

104. Disconnect, for its desktop browser extensions, has announced a general policy of unblocking any ad tracking website that commits to respect users’ DNT designations and to comply with the DNT rules and policies established by EFF, or other comparable organizations. But Google unequivocally refuses to honor user “Do-Not-Track” requests or to implement a Do-Not-Track policy, stating on its official site: “At this time, most web services, including Google’s, do not alter their behavior or change their services upon receiving Do Not Track requests.”

105. In any case, as the Eurecom study observed, the DNT mechanism is restricted to web browsers, and does not work with mobile apps, the means used by most people to engage the internet on mobile devices. Disconnect’s technology bridges this shortcoming – it blocks invisible network connections and tracking by and through mobile apps. As we explain in greater detail below, Google has removed Disconnect’s technology from the Play Store, precisely because it gives the user greater protection from unwanted and potentially malicious invisible tracking on mobile devices.

106. Google is using the full weight of its market power to deny users control over tracking, particularly mobile tracking. The company refuses to honor DNT. It has removed Disconnect’s key technology from the Play Store. And, through its dominant platforms, Google foists on the public a set of privacy and security “features” that do next to nothing to protect the users. Instead, the Google “features” enable the company to continue to gather personal data from its users, which then enables Google to more effectively target its next round of advertising.

140 See, https://www.eff.org/dnt-policy.
142 https://disconnect.me/help#does-disconnect-block-all-ads-is-it-an-adblocker
143 https://support.google.com/chrome/answer/2790761?hl=en
4. Google’s Market Power

107. Google, Inc. is a United States-based multi-national corporation headquartered in Mountain View, California. Google started as a search engine company, engaged in the business of helping users find information on the internet. But, as explained more extensively elsewhere in this Complaint, Google’s business now consists almost entirely of gathering data about the preferences, locations, and behavior of ordinary people and monetizing that data through the sale of targeted advertisements on the internet.

108. Google has a dominant position in providing general online search services throughout the EEA, with market shares above 90% in most EEA countries. On April 15, 2015, the European Commission sent Google a Statement of Objections outlining the Commission’s preliminary view that the company is abusing a dominant position, in breach of EU antitrust rules, by systematically favoring its own comparison shopping product in its general search results pages in the EEA.145

109. The Commission also opened formal proceedings against Google to investigate (among other things) if, by abusing a possible dominant position, Google has illegally hindered the development and market access of mobile communication applications and services in the EEA – by (among other things) tying or bundling certain Google applications and services distributed on Android devices with other Google applications or services.146

4.1. Ad tech and profiling

110. Initially, Google capitalized on its dominance in general online search services to sell ads related to searches. But in April of 2007, Google purchased DoubleClick, Inc., an online advertising company that “derived its value from having profiles on visitors to the net’s most popular sites and letting companies target their ads.”147 As a result of the acquisition, Google secured the capability to target ads to users who had demonstrated an interest in content related to an ad, even when the user was on a webpage that had nothing to do with the advertiser’s product.148 DoubleClick works with both advertisers and publishers.149

111. Shortly before its acquisition by Google, DoubleClick had announced that it had developed a new system for the buying and selling of online ads – an “ad exchange.” Google acquired this new system as part of the DoubleClick deal. The exchange differed from ad auctions that Google had previously used on its networks because the exchange was open to any web publisher or ad network, rather than just the sites on Google’s network.150 The open nature of the exchange permitted a far larger number of parties to track users through Google’s network and for Google, in turn, to track far more users.

147 http://www.wired.com/2009/03/google-ad-annou/
149 http://www.quora.com/How-is-Adsense-different-from-DoubleClick-or-Admob
150 http://www.nytimes.com/2007/04/14/technology/14DoubleClick.html
112. In March of 2009, in a change of policy, Google announced that it would start selling “behavioral profiling ads” (what Google calls “interest-based advertising”). In practical terms, this meant that Google started tracking the online moves of users and combining all of the company’s data to build a collection of interests — a profile — for each user, whether the user had a Google account or not. It was and continues to be necessary for Google to track users and build profiles in order to maximize profits. As explained above, ads that are targeted to the interests of the particular user have higher response rates and Google can therefore charge more for them.

113. On its current website, Google states that ads presented by Google to the user, as he visits sites on the web, are determined by, among other things, the websites the user has previously visited and the apps the user has on his mobile device. Today, the company makes about 90 percent of its revenue from advertising. But management is under enormous pressure from investors and analysts to increase the effectiveness of user tracking in order to increase both revenues and margins.

114. As we have previously explained by reference to the Senate Report, since Google’s acquisition of DoubleClick, the system for the sale and delivery of real-time online advertising has become increasingly complex. There are now six critical advertising technology (“ad tech”) markets: ad networks, ad exchanges, demand-side platforms, supply-side platforms, ad servers and analytics platforms. Through a combination of acquisitions and anticompetitive conduct (including bundling, contractual restrictions and the like), “Google is now the largest and/or dominant player in each.”

115. Indeed, “Google now locks in publishers and advertisers at both ends. It ties services that advertisers or publishers do not want to those that they need, pressuring them to use Google-only services all the way up and down the pipeline.” Google’s anticompetitive efforts have been successful. According to a study recently published by the world’s largest educational and scientific computing society (the Association for Computing Machinery), “Google is dominant in terms of revenue and reach” in the online advertising industry “with presence on 80% of publishers,” based on data from millions of users across multiple networks.

116. Mobile application advertising is an important component of Google’s overall strategy. In 2010, Google bought AdMob, a mobile advertising application network. We discuss the operation and significance of AdMob below.

[152] https://support.google.com/ads/answer/1634057?hl=en&ref_topic=2971788
4.2. The mobile platform

117. Google in August 2005 acquired a startup called “Android, Inc.” which was already working on an operating system for mobile phones. Apple, Inc. introduced the iPhone in early 2007. In part, Google feared that a strong market position by Apple in mobile would lead to Google Search being locked out. More importantly, Google also wanted to create a mobile advertising platform. So, Google announced its own mobile operating system called “Android” later the same year. In order to encourage adoption by handset makers and app creation by developers, Google made Android an “open source project,” meaning that handset makers and app developers could use the Android code without Google’s permission.

4.2.1. Mobile applications

118. The mobile operating system market (like the desktop operating system market) is characterized by powerful network effects, economies of scale, barriers to entry and interdependencies with application software (and other functionality). Users want their smartphones to provide a wide array of functions and will therefore select phones with operating systems for which a wide variety of mobile applications have been written, and in particular, those that have the applications users value the most. “[W]hat every customer expects is for their device to be a platform,” explained one industry executive in the New York Times.

119. In most of these respects, the mobile operating system market is very similar to the desktop operating system market at an earlier point in time. Perhaps the most complete discussion of these factors and their antitrust significance can be found in the trial judge’s decision in the Microsoft case in the U.S. In that decision, after a lengthy trial and based on an enormous trial record created by the United States government, the judge explained how a vast number of application programs entrenches the company that controls the platform’s operating system by creating a barrier to successful entry by rivals and by “locking in” users to keep them from switching to other operating systems.

120. To enhance the value of its mobile OS to handset makers and users, Google created a few proprietary apps for its new mobile platform – mostly clients for Google’s popular online services, including Gmail, Maps and YouTube. Google also created and supported open source applications for Android, including Music, Calendar, and Messaging. And Google

quickly released a software developers’ toolkit (SDK) to make the platform attractive to third party developers.

121. Generally speaking, desktop operating system companies made very little effort to control and facilitate the distribution of third party applications that ran on their platforms.\textsuperscript{165} By contrast, in apparent recognition of the importance of apps to the success of the OS platform, all mobile operating system companies have set up official, curated collections of mobile applications that run on their platforms. These collections are known as “stores.” Operating system companies heavily promote their stores – and specifically the number of applications in their stores -- to consumers as measures of the importance and desirability of the underlying operating system and the hardware on which it is running.

122. In the fall of 2008, Google officially launched its version, the “Android Market.”\textsuperscript{166} We discuss the significance of the Google mobile application store, as it relates to Disconnect, below.

4.2.2. Fragmentation

123. Google’s efforts (through open source and app creation strategies) to secure adoption of its new OS were wildly successful. Android quickly commanded almost 80% of the mobile operating system market.\textsuperscript{167} But initially hardware manufacturers frequently customized the Android operating system to one degree or another, as they deployed it on new devices. This produced enormous “fragmentation” within the platform. Differences in the “skin” of various manufacturers – i.e., differences in packaging and external interfaces – further exacerbated this fragmentation.

124. The Android Software Development Kit (SDK) was intended to facilitate the creation of mobile applications for the platform. But with more than 1600 separate devices running an operating system that differed from one device to another, interoperability became a major issue.\textsuperscript{168}

125. Fragmentation created several problems for Google. First, Android developers had to spend an inordinate amount of time on testing and debugging for disparate hardware platforms, reducing both the profitability of developing on Android and the incentive to develop Android apps in the first place. More importantly to Google, the “openness” of Android and the resulting fragmentation raised the prospect that a handset maker or rival could “fork” the code – use the open code and its attendant apps without Google’s permission to create a competing “Android” platform over which the rival could exercise control by insinuating its own proprietary features and functions.\textsuperscript{169}

\textsuperscript{166} http://venturebeat.com/2008/10/22/google-releases-details-on-android-market-launch/
\textsuperscript{167} http://arstechnica.com/gadgets/2013/10/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/1/
\textsuperscript{168} See, e.g., http://www.droidreport.com/android-fragmentation-concerns-3356 .
\textsuperscript{169} http://arstechnica.com/gadgets/2013/10/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/1/
126. Either outcome – a fragmented platform including many different OS versions or a mobile platform based on Android code but controlled by a rival – would impede Google’s ability to control advertising on the mobile platform and to monetize its market position in mobile through its otherwise dominant “ad tech” system. So, Google developed a plan to convert what was nominally an “open” Android platform with enormous market share into an “ecosystem” that Google could control and monetize. Google’s plan initially focused on control of the applications layer for Android.

127. Google set out to make the application layer into a dominant, proprietary platform in its own right, through which Google could monetize advertising, control the Android operating system and prevent the OEMs from “forking” it. Google already controlled key proprietary apps that it created from its online services – YouTube, Maps, and Gmail, as examples – without which a handset maker could not bring a device to market successfully. It placed those apps into its Store. Next, Google developed proprietary versions of the open source apps running on the open source Android OS, and ceased development of the open sourced versions of the apps, turning them into “abandonware.” Google placed these newly proprietary apps into its Store.

4.2.3. Consolidation techniques

128. Google then devised a scheme to move application developers working with Android’s open interfaces to a dependence on Google’s proprietary interfaces and technology. Google created new developer tools, libraries, services, and APIs (application programmer interfaces) all designed to centralize application development through Google’s mobile application Store. These new services, tools and interfaces were consolidated into a few facilities, among them the “Google Play Developer Console” (for the Google Play Store) and “Google Play Services.”

129. Google has increasingly taken services, functions and interfaces (APIs) out of the operating system and put them into one of these centralizing facilities instead. Google Play Services covers lower level APIs and background services while the Store serves to decouple non-system applications from the operating system. Indeed, in March of 2012, Google even changed the name of its app store from the Android Market to the Google Play Store, severing the association with Android.

130. By the fall of 2013, the press reported that Google had moved all interfaces, libraries, tools, services and functionality from the operating system to ether Play Services or the Play Store, to

---

172 http://arc.applause.com/2014/12/16/google-play-past-present-future/
173 http://www.androidcentral.com/new-google-play-services
175 http://googleblog.blogspot.com/2012/03/introducing-google-play-all-your.html
the extent technically possible. Google even packaged Play Services as an app and put it into the Store. 176

131. Mobile app developers want to reach as wide an audience as possible for their applications, with as small an expenditure of resources as possible. Because Google’s centralizing features permit developers to reach (nearly) the entirety of the Android installed base (including devices running almost all prior Android OS versions released by Google) in one development effort, mobile developers adopted the interfaces, tools, etc. in Play Services and the Play Developer Console, notwithstanding the future dependency on Google. 177

132. Google made adopting its proprietary APIs in Play Services and the Play Developer’s Console even more attractive to mobile developers by making sure that 90% of its APIs worked on Apple’s mobile platform, iOS. Generally speaking, an application written for one operating system will not work on another operating system without substantial modification. By supporting 90% of Apple’s APIs, Google reduced development efforts for any developer already (or wishing to be) on Apple’s mobile platform. This made it even more attractive to develop for Google’s proprietary platform over a forked Android platform or a rival’s platform (other than Apple). 178

133. Google’s strategy to lock developers into its proprietary interfaces worked. Today, Google’s mobile application store has more than 1,500,000 apps – more than any other rival. 179

4.2.4. Mobile OS market power

134. Google used the market power from its mobile applications developed from online services – like Gmail, YouTube, and Maps – along with the market power Google consolidated into its app Store, to gain and maintain control of the nominally “open” Android platform. First, Google apps that are built using the Play Services APIs won’t run on the Android OS without the presence of Play Services. So, a device manufacturer using forked Android code would have to provide a new set of APIs and convince developers to write to them. 180

135. Google also used anticompetitive contractual provisions to keep rivals from forking the Android code. Basically, Google formed a group of the major handset manufacturers called the “Open Handset Alliance.” In order to get Google apps, these manufacturers must agree to only build Google-approved devices. These devices must pass Google’s compatibility tests, meaning that they must run all apps in the Google’s app store. So, at bottom, the manufacturers are agreeing not to fork the Android code. 181


179 http://www.appbrain.com/stats/number-of-android-apps


136. Google’s efforts to exert control over the Android operating system platform were successful. Google’s Play Services now runs on just about every Android device.182 A couple of firms, Alibaba and Amazon, have used the open source version of Android (without a contract with Google) to power smartphones, but these devices have had limited commercial success.183 The Google-controlled versions of Android constitute the entirety, more or less, of the Android “market.”184

137. The Android OS, controlled by Google, dominates the market for mobile operating systems. Market share figures show “very strong evidence” of dominance. IDC provides smartphone and tablet shipment data by OS. Data is available at a worldwide level, as well as for certain countries. 17 of the 31 EEA countries are tracked, and these comprise 88% of the total EEA population.

138. Worldwide, in the first quarter of 2014, Android’s share of shipped smartphones was 81%, and its share of shipped tablets was 65%. Due to the higher number of shipped smartphones than tablets, this puts Android’s share of all shipped smartphones and tablets combined worldwide at 79%. In the EEA, Android’s share is slightly lower: 74% for smartphones, 67% for tablets, and a combined smartphones and tablet share of 72%.

139. The vast number of applications written to run on Android, coupled with Google’s anticompetitive contracting provisions, constitutes a formidable barrier to the market entry of rival mobile operating systems. As indicated above, competitors using open source versions of Android have failed. Similarly, although Google’s rivals, including Microsoft, Samsung, Firefox and Cyanogen, have attempted to enter the mobile OS market, they have relatively little distribution.185

4.3. Market power over mobile apps

140. Google has used its control of the operating system to further bolster the market dominance of its mobile application Store. Through the technique of “full line forcing,” Google ensures that the application Store is tied to Android distribution, thereby transferring Android’s market share and market power to Google’s application store. Device makers that want to build a mobile phone running the latest version of Android (and particularly if they want to include any Google services or applications) must sign a contract with Google known as the Mobile Application Distribution Agreement (MADA). The version of Android that they get from Google (version 2.2 and above) comes with the Play Store application already installed, a requirement

---

183 https://www.theinformation.com/Google-s-Confidential-Android-Contracts-Show-Rising-Requirements
that Google makes no efforts to conceal.\textsuperscript{186} In fact, MADA usually specifies that the icon for the Google Play App store appear on or adjacent to the “default home screen” of the device.\textsuperscript{187}

141. The net result of these contractual restrictions is that the market share and market power of Google’s mobile application store can fairly be inferred from Android’s market share and market power. This is particularly true from the developer’s perspective. There is no way for a developer to write an app to run on Android, meaning on more than 70% of the market, without access to and participation in the Play Store, and the various development interfaces and technologies it contains.

142. The utility of available data on mobile app store market shares is limited, as we explain below. But as limited as these studies are, they nevertheless show shares for the Google application store in a range that is “indicative” of dominance. For example, there is an EU study using data from IHS that shows Google’s mobile app store as the worldwide leader in downloads, with about 45%, based on what looks to be 2012 or 2013 data. The study projects download numbers from the Google app store increasing rapidly, with the attendant increase in market share, to roughly 75% as an estimate for 2015.\textsuperscript{188}

143. This kind of study is not usually helpful in determining either market power or the benefit conferred upon an app by participation in one particular app store as opposed to another. These studies are generally based on historical data and therefore overestimate the current popularity of app stores that started before Google’s. Also, for a variety of reasons, owners of Apple mobile phones historically downloaded more apps than owners of Android phones (although this is changing), further distorting the data. Whatever the number of downloads attributable historically to any particular app store, the market shares of Android and its mobile operating system competitors make it clear that if a developer could not operate on the Android platform, its market penetration would be capped at less than 30% of mobile phones.

4.3.1. Market power over app developers

144. Google used its control over its app Store and its market power over mobile app distribution to discipline, control and exclude potential mobile operating system rivals from the mobile OS market, as we have explained above. In addition, Google has used the market power in mobile app distribution it created to discipline and otherwise control app developers by making participation in the Play Store the gating process for access to the market of potential customers – i.e., Android device users. According to Google, “Google Play now reaches more than 1 billion people on Android devices in more than 190 countries.”\textsuperscript{189}

145. To create apps for the Android platform, a developer, among other things, must create a Google Developer Account,\textsuperscript{190} and must sign the Android Software Development Kit License

\textsuperscript{186} https://support.google.com/googleplay/answer/190860?hl=en
\textsuperscript{187} http://www.benedelman.org/news/021314-1.html
\textsuperscript{189} http://android-developers.blogspot.com/2015/02/a-new-way-to-promote-your-app-on-google.html
\textsuperscript{190} https://support.google.com/googleplay/android-developer/answer/6112435?hl=en
Agreement. Through this agreement, Google provides the developer with the files, APIs and information necessary to create an app that runs on Android.

146. To publish the Android apps the developer has created through the Play Store, the developer must, among other things, sign an additional agreement, the Google Play Developer Distribution Agreement. Through this second agreement, the developer can secure placement in the Play Store, as well as additional APIs, benefits and information to create and publish Android apps. To actually publish and distribute an app through the Play Store, the developer must register the application (individually) in the Google Play Developer Console. Google “approves” an app that the developer registers by issuing “authentication tokens” or “keys” for that app. These tokens, among other things, provide access to APIs. If Google approves the app, it is published in the Play Store.

147. By placing particular mobile applications in its store, Google confers the imprimatur of its brand on the selected applications, making the applications considerably more desirable to consumers. Google also provides additional marketing and distribution services, not otherwise available, to applications included in the Play Store. For example, Google provides search (by keyword) and browsing (by category) functionality that enables consumers to quickly identify and locate for downloading applications in the Play Store that they are interested in. Through a variety of curation devices, Google enables users to access the quality of applications and decide which are best suited to satisfy a particular interest.

148. Google also provides consumers with an easy way to download the apps they want directly to their phones, and to pay for those apps (for which there is a fee). And, finally, Google provides applications in the Play Store with access to certain functionality that Google does not make available to applications outside the store. The importance of these functionalities and services to app developers is described in greater detail below.

149. The actual and threatened denial of these essential technologies and services disciplines app developers in terms of the features and functions they provide to consumers. Google can rescind authorization at any time for an app published in the Play Store by taking the position that the developer or the app are violating a provision of one of the agreements signed by the developer. Google “unpublishes” the app by removing it from the Play Store and invalidating the relevant authorization tokens. Under circumstances (vaguely) specified in the written agreements, Google can also terminate the developer’s Google Play developer account, the developer’s Google developer account and related Google accounts, and recover the proceeds and costs associated with past sales of the app. So, Google can use its market power to make certain that consumers only get the technology that Google wants them to get.

4.3.2. Monetization of market power

150. A large number of applications in the Play Store are available without charge – for free. Other apps in the Play Store use a standard paid application model, or a “freemium” model, in which

---

192 [https://play.google.com/about/developer-distribution-agreement.html](https://play.google.com/about/developer-distribution-agreement.html)
the basic product is free, but in-app purchases of other products or upgrades of the basic product are offered through the Play Store for a fee, from which Google takes a percentage.\footnote{\url{http://www.androidauthority.com/how-to-monetize-android-app-379638/}} So, Google secures revenue through the Play Store by charging application vendors for participation in the Store and by taking a percentage of the fee charged for those applications that are not free. But this revenue pales in comparison to the money Google makes from advertising on mobile apps.

151. Both free applications and many of those that charge a fee for downloading usually make money by hosting advertising that is displayed when the app is opened on the user’s screen. The application developer is usually compensated by the mobile application advertising network hosting the ad on a CTR (click-through-rate) basis. As mentioned above, “AdMob” (a company acquired in 2010) is Google’s mobile application advertising network.\footnote{\url{https://developers.google.com/monetize/}} Today, AdMob is the largest mobile advertising network on the Android platform (i.e., for Play Store apps) by far; it faces only fringe competition.\footnote{\url{http://www.appbrain.com/stats/libraries/ad}}

152. AdMob allows mobile app developers to monetize their apps and promote them. AdMob acts as both a publisher ad network and a buying ad network. As a publisher ad network, it enables mobile developers to make money by selling ads (which are displayed in their apps) served by different ad networks (including DoubleClick).\footnote{\url{http://www.quora.com/How-is-AdSense-different-from-DoubleClick-or-Admob}} Originally, developers used the AdMob Software Developers’ Kit to access AdMob’s capabilities. But starting last year, access to AdMob was folded into and provided through the Google Mobile Apps SDK, which is part of Google Play Services.\footnote{\url{https://developer.android.com/google/play-services/ads.html}}

153. The acquisition of AdMob permitted Google to execute the same monetization strategy that it had successfully used on the desktop. For example, Google can use the knowledge (gained through control of the Play Store) that a user has downloaded a particular mobile app to target ads to that user inside other mobile applications that use AdMob and therefore charge more for the ad. More generally, Google can use the mobile apps it owns, AdMob and DoubleClick) to track users as they use their mobile devices and use that information to target ads hosted by mobile apps.

4.4. Market power in the Chrome Mobile Browser

154. Google has used its market power from both Android and the Play Store to leverage some of its other products – most strategically, its proprietary Chrome browser – to market dominance. Originally, the open source Android OS code came with a stock, default, open source browser (the “Android browser”) pre-installed.\footnote{\url{http://www.mobilexweb.com/blog/android-browser-eternal-dying}} As part of its plan to close its platform, Google stopped development on the stock Android browser in favor of its proprietary Chrome
browser.\textsuperscript{199} Starting roughly two years ago, Google began to bundle its proprietary Chrome browser pre-installed as the default stock browser with the Android OS code, instead of the old open source Android browser.\textsuperscript{200}

155. The Chrome mobile browser is also available as a standalone app and as an app in the Play Store. Device makers are required by contract with Google to carry both the Store app and the Chrome Bowser app on their devices, and to display the icons for the Store and the Chrome browser prominently to users.\textsuperscript{201}

156. Google’s efforts at leverage through the Android OS and the Play Store have been successful in establishing market power in the Chrome mobile browser. The most current available data indicates that Google’s browsers account for more than 60% of the mobile browser market in Europe. More than two-thirds of Google’s share is attributable to the proprietary Chrome mobile browser. Furthermore, the overall market share attributable to the proprietary Chrome mobile browser is rising rapidly, at the expense of the two closest market participants – the old Android browser that Google formerly bundled, and Apple’s Safari browser.\textsuperscript{202}

4.5. Abuse of dominant positions

157. Google has abused its dominant positions with respect to the Android mobile OS, the Play Store and the Chrome mobile browser in two principal ways. First, Google has technologically integrated its own ineffective privacy and security “features” into its dominant products, thereby giving itself an unfair market advantage and harming consumers in the process. Second, Google has used its market power to discriminate against Disconnect and otherwise to impede Disconnect’s access to customers by removing Disconnect’s award-winning technology from the Play Store, and by denying the company necessary technical information and distribution without proper justification.

\begin{itemize}
\item \textsuperscript{199} \url{http://arstechnica.com/gadgets/2013/10/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/2/}
\item \textsuperscript{200} \url{http://download.cnet.com/Chrome-for-Android/3000-2356_4-75650330.html}
\item \textsuperscript{201} \url{https://www.theinformation.com/Googles-Confidential-Android-Contracts-Show-Rising-Requirements}
\item \textsuperscript{202} \url{http://gs.statcounter.com/#mobile_browser-eu-monthly-201001-201505}
\end{itemize}
5. **Google’s Privacy and Security Software**

5.1. **Invisible connections**

158. The dispute between Disconnect and Google centers on the invisible and undisclosed network connections that third parties (sites and services other than the one the user is trying to connect to) try to make with the user’s browser or mobile device, frequently without the user’s permission. These invisible connections, as we explain above, permit intrusions into the personal privacy of users by facilitating tracking and the collection of personal information. They also expose users to risks associated with malware and other forms of cybercrime, including identity theft. Disconnect’s technology permits users to disintermediate invisible connections to problematic sites. In effect, Disconnect makes tracking truly consensual and removes the attendant malware risks.

159. But invisible, unsolicited tracking is Google’s lifeblood. The company makes virtually all of its revenue from advertising. Tracking permits Google to target its ads and, hence, to charge advertisers far more for ad placement. Indeed, Google is under enormous pressure from the financial community to increase the “effectiveness” of its tracking, so that it can increase revenues and profits. Giving a user the ability to control his own privacy information (and to protect himself from malware) by blocking invisible connections to problematic sites constitutes an existential threat to Google.

5.2. **Tying**

160. Google has attempted to blunt this threat. As we discuss in subsequent sections, Google has removed Disconnect’s technology from the Play Store, making it all but impossible for the vast majority of mobile users to avail themselves of effective protection. Google has also sought to subvert, obfuscate, and co-opt consumer concerns about internet privacy and security through anticompetitive tying.

161. Basically, Google has incorporated (technically tied) into its dominant products privacy and security functions that mislead the user into thinking he has secured some protection, when in reality these functions leave Google and/or other services free to continue to track. Hence, the risks of tracking and malware remain, largely unabated. The tying practices foist ineffective solutions on the consumer, but nevertheless diminish the market for Disconnect’s more effective solution because many consumers believe themselves to be protected by Google’s bundled features.

5.3. **Privacy**

162. Google has bundled into the Android OS and the Chrome mobile browser privacy features and options that appear to the consumer to compete with Disconnect’s blocking technology. In

---

reality, as we explain below, Google’s features and options do not eliminate the risks to user privacy or security.

5.3.1. Interest-based ads

163. Foremost among Google’s privacy ploys is its bundled function that permits users to opt out of behavioural advertising. Google’s web site (and a Chrome browser extension) permits the user to opt out of a certain limited group of “interested-based” ads on Google and across the web through a set of menus. This feature allows the user to opt out of ads that are shown by Google to the user based on the user’s “interests, previous visits to other websites and demographic details” stored on the user’s browser.

164. The option is confusing, at best. The instructions for invoking the opt-out option state that the opt out requires cookie-based tracking to function; the opt out will not work where cookies are not used, such as in mobile applications.204 And on the same page, Google admits that it uses “identifiers” (e.g., fingerprinting) other than cookies, but that perform “similar functions to cookies,” in order to serve targeted ads in mobile apps.205 So, apparently, the basic function to opt out of interest-based ads may not work at all for mobile ads.

165. Nevertheless, a version of this limited opt-out feature is bundled into the dominant Android operating system through the “Google Settings/Ads” webpage. But it is even more limited than the desktop version. By its own terms, the opt-out feature in Android does not stop the placement of ads based on the user’s Google Profile by certain key Google apps, including YouTube and Maps for Mobile. Nor does it enable opting out of “interest-based” ads on the many mobile apps (including those in the Google Play Store) that allow the user to view web pages without launching the mobile device’s default web browser. All of these limitations can only be viewed by visiting the URL in the footnote while on Android Chrome.206

166. In any event, both the mobile “opt-out” feature and the desktop “opt-out” feature are subject to more fundamental criticisms. Invoking the “opt out” feature on either mobile or the desktop only stops Google from showing the user “interest-based” ads. Google still targets the user with non-interest based ads, such as “context-based” ads (i.e., ads targeted based on the site the user is on, the user’s geographic location, recent searches, and other non-interest-based data).207 So, the user’s risk of exposure to malvertising remains largely unabated.

167. Nor does invoking the opt-out feature prevent companies other than Google from targeting the user with “interest based” ads. Even with the feature invoked, a user browsing the internet (or opening mobile applications, to the extent the option applies to mobile apps) will see interest-based ads from companies other than Google.208 Most importantly, the feature does not prevent Google or any other company from tracking the user; it only prevents Google from

204 https://support.google.com/ads/answer/2662922?hl=en
205 https://support.google.com/ads/answer/2662922?hl=en
207 https://support.google.com/ads/answer/2662922?hl=en
208 https://support.google.com/ads/answer/2662922?hl=en
showing the user certain ads. So, the privacy intrusion (as well as the risk of exposure to malware) remains unabated.

168. The European online advertising industry, as represented by the European Advertising Standards Alliance (EASA) and the Internet Advertising Bureau Europe (IAB), have published a website that permits European users to opt out of behavioural advertising on listed member networks.²⁰⁹ This is the same approach Google takes (but Google uses the terminology, “interest-based ads”). Indeed, Google participates in this site and send its own users to this site if they wish to disable other companies’ interest-based ads.²¹⁰

169. The Article 29 Working Party has analyzed this approach to protecting user privacy and found it inconsistent with the revised ePrivacy Directive for several reasons. First and foremost, like Google’s option (that is integrated into Android) to permit mobile users to opt out of “interest-based ads,” opting out of “behavioural advertising” does not stop participating advertising networks from continuing to track users.²¹¹ The Working Party also noted that device identifiers like fingerprinting permit sufficient user identification for tracking, even if other personal data is anonymized.²¹²

5.4. Privacy functions bundled into browser

170. Google incorporates a number of “features” and functions that nominally protect user privacy into its dominant Chrome mobile browser. As we explain below, these bundled functions are of limited utility in actually protecting user privacy. And they are frequently presented to the users in misleading terms, suggesting broader protection than they actually deliver. In any case, these functions only “protect” users of the Chrome mobile browser. Users who open mobile apps directly, for example, would not be covered by the features, nor would users of other browsers.

5.4.1. Incognito Mode

171. Google offers and publicizes a feature called “Incognito Mode.” This feature is bundled into Google’s Chrome browser as well as Google’s Chrome mobile browser.²¹³ According to Google’s description, the user should select Incognito Mode if “you don’t want Google Chrome to save a record of what you visit and download.” The description goes on to state that in Incognito Mode, the user will not “leave browsing history and cookies” on the user’s computer.²¹⁴

172. But, as more astute commentary explains: “Chrome’s ‘Incognito’ might stop Chrome itself from logging your browsing data, but it doesn’t stop your operating system, your router, or the websites themselves from logging that you’re there. When streaming content, whether you’re in ‘Incognito’ mode or not, you open yourself up to data storing, and this mode does not hide

²⁰⁹ http://www.youronlinechoices.com/uk/your-ad-choices
²¹⁰ https://support.google.com/ads/answer/2662922?hl=en
²¹² Opinion 16/2011 at 8.
²¹³ https://support.google.com/chrome/answer/95464?hl=en
²¹⁴ https://support.google.com/chrome/answer/95464?hl=en
your IP address, meaning that information such as your location, your browser, your operating system and even your physical address might still be seen.”

173. Google even admits some of these limitations: “Neither Incognito mode nor Guest mode makes you invisible on the web. Websites you visit, your employer, or your service provider can still see your browsing activity.” So, at bottom, while Incognito Mode may prevent Chrome, a local application on the user’s client, from saving the user’s browsing history (meaning that other users of the same computer cannot see the browsing history), Incognito Mode does not prevent Google servers from detecting and saving the user’s browsing history, nor does it prevent other websites and third parties from tracking the user, especially if the user is logged into an account by name.

5.4.2. Delete Browsing activity

174. Google’s Chrome desktop browser and the mobile version bundled with Android both include a “Delete Search and Browsing Activity” function that covers Android apps. Users who read the “fine print” will learn that invoking this function does not delete tracking information that Google has complied on a user. The Google site states that this “delete” function only works when the user is logged into a Google account and only stops “deleted” items from being associated with the user’s Google account. But the tracking information compiled by Google is not associated with user accounts in the first place and therefore is not subject to this “delete” function.

175. In fact, Google cautions the user that the company stores browsing activity “separately” in order to “improve our services.” Google’s “services” include AdWords, AdSense, AdMob, and Google Analytics, among other services. So, without actually being forthright, Google is reserving the right to use the browsing history for “targeting” “interest-based ads,” and more broadly tracking the user to identify him and compile profiles.

5.4.3. Blocking cookies

176. Through a complex set of maneuvers, a bundled feature in the Chrome browser permits the user to block all (or just third-party) cookies by default. (Google will even permit the user to opt out of the DoubleClick cookie permanently, using a browser plug-in.) This feature is confined to “cookies.” As the Article 29 Working Party observed, flash cookies are generally impervious to the traditional privacy settings of a web browser, as is fingerprinting. So,
this browser function does not prevent Google or any other tracking service from tracking and targeting the user via means other than cookies.

177. Despite the fact that many mobile devices may not use cookies, the Chrome mobile browser also has a bundled function to “block third party cookies and site data.” It is unclear what, if any, privacy “protection” this setting invokes. Manifestly, it does not claim to block tracking.

5.4.4. Effect of bundling

178. Google’s various user privacy features are largely ineffective. But they are presented to the user in ways that suggest the user can get more privacy protection from them than is actually the case. Google’s efforts to confound users seeking to protect their privacy have been successful, at least in the United States. A couple of years ago, a user survey by a well-respected nonpartisan, not-for-profit, public interest group found that only 38% of U.S. internet users were even “generally aware” of ways to limit data collection by websites.

179. More tellingly, 81% of this group (the 38%) sought to limit personal data collection by deleting their web histories, and 65% tried to limit data collection by changing their browser settings. As shown above, executing these two techniques on Google sites and products do little to limit the collection of personal information.

5.5. Malvertising

180. In addition to creating personal privacy issues, invisible network connections – including those between third party ad servers and the user’s browser or mobile device – can be used both to distribute malware and to collect user information for malicious (as opposed to advertising) purposes. In other words, cybercriminals can use online advertisements and advertising technology to exploit the same kinds of invisible network connections used by advertising networks for tracking.

181. Google has known since at least 2006 that ads are being used to distribute malware. More recently, a Google executive told the U.S. Senate Committee that published the report on malvertising that cybercriminals use online advertising to distribute malware in various ways, including “malicious code hidden within an ad creative ... embedded on a webpage , or within software downloads.”

5.5.1. Google’s true interests

182. Google makes almost all of its revenue from online advertising. Its interests therefore lie in publishing as many ads as possible, even if some or even a substantial number, are corrupted. From Google’s viewpoint, it is better to publish the ads and collect the revenue first, and deal

225 http://www.pewinternet.org/2012/03/09/search-engine-use-2012/
226 http://googleonlinesecurity.blogspot.com/2008/02/all-your-iframes-are-point-to-us.html
with malware effects on consumers only later (if at all). Hence, Google’s efforts to deal with malvertising have been half-hearted – more correctly, disingenuous.

183. Disconnect’s technology protects users from malvertising quite effectively. But as with privacy protection, providing users with protection from malvertising costs Google money. So, as with privacy protection, Google has made Disconnect’s solution hard for consumers to obtain, while insinuating its own less effective “protection,” frequently by tying.

5.5.2. Safe browsing

184. According to the Google executive who testified at the Senate malvertising hearings, Google takes a two-pronged approach to protecting users from malware. Malvertising Hearings at p. 60. First, Google attempts to prevent users “from accessing infected sites altogether” using what it calls “Safe Browsing,” which it first deployed in 2006. In reality, “Safe Browsing” is nothing more than a continuously updated list of “known” malware (and phishing) sites.228

185. Google creates and updates the list by examining “billions of URLs per day” looking for “attack sites” (that hackers use to distribute malicious software) and “compromised sites” (formerly legitimate sites that have been hacked to include malicious software).229 The Senate Report explains that this approach is only modestly effective (something Google must have surely known for years) because the actual file at a particular URL can be “quietly changed after that initial quality control check” from an innocuous and safe site to “a vehicle for malware” at the time the user accesses it.230

186. This modestly effective Safe Browsing “feature” is bundled into Google’s Chrome desktop browser and set as the default.231 When a user navigates directly to a compromised site or is directed to one through an advertisement, the browser posts a warning to the user.232 Google also makes the list available to application developers through an API.233

187. Google’s site says that Safe Browsing is not yet supported in the Chrome mobile browser.234 But testing using the URL Google designates to enable users to determine if Safe Browsing works shows the feature to be active in the Chrome mobile browser.235 In any case, the feature is no more effective on mobile than on the desktop.

---

228 Malvertising Hearings at p. 61.
229 http://www.google.com/transparencyreport/safebrowsing/
230 Senate Report at p. 15.
231 https://support.google.com/chrome/answer/99020?hl=en
232 Malvertising Hearings at p. 62.
233 https://developers.google.com/safe-browsing/
234 https://support.google.com/chrome/answer/2440264?hl=en
5.5.3. “Anti-malvertising” site

188. In 2009, Google also launched an informational site designed to help publishers, ad operators, and users avoid malvertising.\(^\text{236}\) The site contains a search mechanism to enable publishers to conduct background checks on prospective partners as well as tips for users and others to avoid malvertising, but it does not contain any functionality to protect users from exposure to contaminated sites. According to the press, Google launched the site to stop ad blocking from becoming a standard security practice.\(^\text{237}\)

5.5.4. Ad scanning

189. The second “prong” of Google’s approach to malvertising involves a combination of contractual prohibitions and ad scanning. Google’s contract terms prohibit advertisers from distributing malware.\(^\text{238}\) Violations (if they can be documented and associated with a particular account) result in suspension.\(^\text{239}\)

190. The more important part of the second prong is a system Google deployed in 2006 to scan ads in its advertising services for malware and disable accounts that distribute malware. Some ads – those “that pose the greatest risk to users” – are rescanned after initial vetting.\(^\text{240}\) But the Senate Report found that such scanning is “ineffective” at preventing malvertising because cybercriminals direct malicious advertisements away from the geographic location of scanners or change a benign advertisement into malware after it has been scanned and cleared.\(^\text{241}\)

5.6. Google’s techniques ineffective

191. Given the flawed techniques knowingly employed by Google, the company, not surprisingly, has been spectacularly ineffective at protecting users from malvertising. Indeed, Google’s sites and ad networks are frequently linked to malvertising incidents that have caused widespread consumer injury.

5.6.1. YouTube

192. For example, the Senate Report described an incident in February of 2014 in which malware was delivered though Google’s ad network to users on YouTube (owned by Google). In that attack, consumers’ computers could become infected with a virus that broke into online bank accounts merely by watching a YouTube video; they did not even have to click on the ad.\(^\text{242}\) YouTube users were targeted with a similar attack in 2013.\(^\text{243}\) And in September of 2014, YouTube was caught publishing malicious ads on videos with more than 11 million views.\(^\text{244}\)

\(^{236}\) http://www.anti-malvertising.com/ResearchEngine
\(^{238}\) https://adwords.google.com/select/tsandcsfinder
\(^{239}\) Malvertising Hearings at p. 63.
\(^{240}\) Malvertising Hearings at p. 63.
\(^{241}\) Senate Report at p. 6.
\(^{242}\) Senate Report at p. 24.
\(^{243}\) Malvertising Hearings at p. 63.
\(^{244}\) http://labs.bromium.com/2014/02/21/the-wild-wild-web-youtube-ads-serving-malware/
http://www.computerworld.com/article/2833934/youtube-served-malicious-ads.html
5.6.2. **DoubleClick**

193. Google’s DoubleClick ad network has been compromised with even greater frequency. In addition to the 2014 incident described in the Senate Report, the Register (UK) has reported that DoubleClick “has repeatedly been caught” distributing malicious ads on the sites of unwitting publishers, citing incidents in 2007 and 2009.\(^{245}\) In December of 2010, the press reported that DoubleClick was caught “pushing ads that linked to a malicious site.”\(^{246}\) Similar incidents were reported in 2014.\(^{247}\)

5.6.3. **AdMob**

194. AdMob, owned by Google, is the largest mobile advertising network on the Android platform.\(^{248}\) According to a detailed analysis published in the McAfee Mobile Security Report in February of 2014, AdMob has “a track record of being associated with malware” and is one of the “favorites of malware authors.”\(^{249}\)

5.6.4. **Google’s Play Store**

195. Google’s Play Store, like the company’s official sites and advertising networks, is also a persistent source of malware dangers to consumers.\(^{250}\) In 2011, following years of criticism about mobile applications in Google’s app store that stole user data and engaged in other abuses, the company deployed a scanning system (much like its ineffective advertising scanning) to check apps in its Store (then known as Android Market) for malware and abusive behavior. The company scanned each application when it was first uploaded to the Store and periodically thereafter.

196. But a few months after the system’s deployment, independent researchers found at least 22 malicious apps in the Android Market, some of which had been downloaded more than 10,000 times.\(^{251}\) A few months later in June 2012, mobile security experts announced that they had devised “multiple ways” to avoid Google’s scanning system.\(^{252}\)

197. Many of the malware dangers to consumers emanating from the Google Play Store have been associated with malicious advertising. For example, in 2013, the press reported that at least 35 apps in Google’s Store – that had been downloaded from two million to nine million times over

---

\(^{245}\) [http://www.theregister.co.uk/2009/02/24/doubleclick_distributes_malware/](http://www.theregister.co.uk/2009/02/24/doubleclick_distributes_malware/)


\(^{248}\) [http://www.appbrain.com/stats/libraries/ad](http://www.appbrain.com/stats/libraries/ad)


\(^{252}\) [http://arstechnica.com/security/2012/06/android-bouncer_bypass/](http://arstechnica.com/security/2012/06/android-bouncer_bypass/)
a 10 month period – were infected with a “malicious ad network library” that uploaded phone numbers and unique device identifiers.\textsuperscript{253}

198. And earlier this year (2015), the computer press reported that some of the apps in the Play Store that had been “downloaded by millions of Android users” displayed fake ads that redirected the users to “harmful threats,” such as apps that collect unwarranted amounts of personal data. Notwithstanding the company’s obviously ineffective prophylactic efforts, the article concluded, “[T]here’s no way to know for sure an app available in Play isn’t malicious.”\textsuperscript{254}

5.6.5. Google’s true intentions

199. Like Google’s half-hearted approach to malvertising, the company’s lackadaisical response to malware distribution through the Play Store is by design. Google makes enormous revenues from advertising on the mobile applications in the Play Store. From Google’s perspective, dealing with malware takes a back seat to distributing apps of “dubious origin,” and collecting the advertising revenue they generate.\textsuperscript{255}

200. The recent Eurecom study of tracking by Play Store apps noted the difference between the stricter vetting procedures employed by Apple for inclusion of mobile applications it is Store – as contrasted with Google’s “much looser set of guidelines.”\textsuperscript{256} Indeed, the Eurecom study concluded that Google’s lack of oversight “makes it all too easy for end-users applications of dubious origin.” Eurecom study at 18. According to the study, Google even awarded its “Top Developer Badge” to several of the apps that connect to a large number of tracking services.\textsuperscript{257}

5.7. Lack of notification to users

201. While Google from time to time publishes reports claiming that it has removed millions of “bad ads” from its system\textsuperscript{258}, the company shows next to no initiative in announcing and warning users about successful malvertising attacks executed through its network (or malware infested apps distributed through the Play Store). Successful malware attacks on Google’s network and Store are invariably revealed by the independent research of security companies like Avast, Trend Micro, Bitdefender, Malwarebytes, Symantec, Bromium Labs, among others, which document the incidents and warn consumers through web postings.

202. These security firms contact Google when they discover a problem. Google invariably acknowledges the problem in vague language and promises to fix it -- after users have already been exposed to malware.\textsuperscript{259} Google’s less than forthright conduct regarding the disclosure of malvertising attacks appears to run afoul of the obligation to promptly inform users about

\begin{itemize}
\item \textsuperscript{253} http://arstechnica.com/security/2013/04/more-badnews-for-android-new-malicious-apps-found-in-google-play/
\item \textsuperscript{254} http://arstechnica.com/security/2015/02/malicious-google-play-apps-may-have-hosed-millions-of-android-handsets/
\item See Eurecom study at 18.
\item \textsuperscript{256} Eurecom study at 1.
\item \textsuperscript{257} Eurecom study at 13.
\item \textsuperscript{258} see http://adwords.blogspot.com/2014/01/busting-bad-advertising-practices-2013.html
\item \textsuperscript{259} See, e.g., http://www.theregister.co.uk/2009/02/24/doubleclick_distributes_malware/
\end{itemize}
personal data breaches, as set forth in the ePrivacy Directive and the various Working Party Opinions.\textsuperscript{260}

\textsuperscript{260} See, e.g., Opinion 2/2013 at 28.
6. **Google’s Exclusionary Conduct**

6.1. **Browser extension**

203. While Disconnect had previously released browser extension products that blocked tracking by a small number of important websites, the company’s release of “Disconnect version 2,” an extension for Google’s Chrome browser and the Firefox browser (and later, Opera and Safari), represented a significant step forward in private browsing functionality. The product, released April 15, 2013, permits users to block more than 2000 tracking sites and services.\(^{261}\)

6.1.1. **Network connections**

204. Basically, the product is engineered to detect when the user’s browser tries to make a connection to a site or server other than the site the user is visiting (i.e., a “third party site”). In technical parlance, such attempts to connect are called “network requests” or “network calls.” If the third party site or server is in a database (or list) Disconnect maintains of invisible, unsolicited, and potentially malicious tracking services, the network connection is blocked.\(^{262}\) Version 2 of the browser extension also includes the company’s web tracking visualization technology.\(^{263}\)

6.1.2. **Block list**

205. Disconnect prepared the tracker database with considerable care. Disconnect started with the list of the web’s 1000 most popular sites created by the well-known analytics company, Alexa (part of Amazon)\(^{264}\), but swapped out some of the non-English and other sites that do not include third party tracking, with popular English language sites that are associated with third party tracking. Disconnect then used a web crawler on the top list’s sites to detect third party requests. Third parties that appeared on more than 1% of the top sites were set aside for analysis. Disconnect placed these third parties into four categories: advertising, analytics, social, and content.

206. The “advertising” category includes services like DoubleClick that invisibly collect personal information and display ads. As previously explained, these ads can expose users to malware, even if the user does not interact with them. The “analytics” category includes companies like Scorecard Research (part of comScore, Inc.) and Google Analytics. These businesses invisibly collect user information and build profiles as users browse the web. As previously explained, these profiles can frequently be connected with users’ real names.

207. A “social widget” is a code snippet provided by social networking services that website publishers embed in their webpages. Social widgets connect back to the social networking service when the widget loads on the webpage. These widgets (e.g., Facebook Like, +1, or

---


\(^{262}\) [https://disconnect.me/help#disconnect-private-browsing-browser-extension_faq](https://disconnect.me/help#disconnect-private-browsing-browser-extension_faq)


Tweet) allow users to interact with a social network from any webpage, but also allow the social networks to track the web browsing activities of users when the users are not on the social network’s domain. And, finally, companies in the “content” category are responsible for the delivery of some content onto webpages that is useful to users (for example, YouTube or Buzzfeed). But they may invisibly collect personal information.

208. Disconnect’s private browsing extension shows the user exactly which tracker sites are attempting to make network connections, and how the company has categorized each one, as illustrated in this screenshot:

![Disconnect private browsing extension screenshot](image)

209. Disconnect uses a combination of user feedback and common sense to decide which sites to block. “Our goal is to ship the perfect balance of privacy, security and usability,” CEO Casey Oppenheim has explained. For the private browsing extension (Disconnect version 2) released in 2013, Disconnect set the product to block network requests from sites/servers in the advertising, analytics and social categories as the default. Sites in the content category were left unblocked as the default because blocking network requests from sites in that category would frequently “break” the site the user was attempting to view.


266 [https://disconnect.me/help#disconnect-private-browsing-browser-extension_faq](https://disconnect.me/help#disconnect-private-browsing-browser-extension_faq)
210. The current list of blocked sites and services can be found here.\textsuperscript{267} It is updated from time to time, of course, and the browser extension automatically uses the updated list.

6.1.3. Operation

211. When a user with the Disconnect private browsing extension installed tries to navigate to a webpage designated by the user, it will load normally. However, attempts by third parties on the block list to make network connections (generally invisible to the user) while the desired page is loading will be disintermediated. So, if an ad from a third party server attempts to load along with the page the user is navigating to, the ad will be blocked (and will not appear) if the third party site or service is on Disconnect’s block list. Of course, this may reduce the revenues of websites that sell space to advertisers.

6.1.4. Treatment of ads

212. But it is important to note that while the Disconnect product sometimes blocks ads, it is not an “ad blocker.” Even with the Disconnect product installed and operating, websites can still make money selling space to advertisers. If the third party serving the ad is not on the block list because it does not facilitate invisible tracking, the ad will load. And whenever possible Disconnect attempts to avoid blocking ads served by the site the user is navigating to (as opposed to third party sites) – so called “first-party ads.”

213. Furthermore, sites have been removed from the company’s block list by Disconnect when circumstances warrant, and the company has a general policy of removing from the block list any company that agrees to adhere to the DNT policy of EFF or a comparable organization.\textsuperscript{268}

6.1.5. Availability

214. Availability: The Disconnect browser extension for private browsing continues to be available for download from the Disconnect site and from the sites of the various browsers with which it works.\textsuperscript{269} For example, the extension for Firefox is available from the Mozilla.org site, which indicates that the product has about 250,000 users and a four star rating.\textsuperscript{270} Similarly, and notwithstanding Google’s anticompetitive action against Disconnect’s mobile malvertising product described below, the Chrome browser extension for private browsing continues to be available from the Chrome Store, and has over 750,000 users with a four and a half star rating.\textsuperscript{271}

6.2. Mobile / malvertising app

215. Extending the company’s private browsing functionality to the mobile platform was no small task. Disconnect’s engineers worked on the problem for more than a year and the company spent $300,000 (US), ultimately developing an application for the leading mobile devices to

\textsuperscript{267} \url{https://disconnect.me/services-plaintext.json}
\textsuperscript{268} \url{https://disconnect.me/help#does-disconnect-block-all-ads-is-it-an-adblocker}
\textsuperscript{269} See, e.g., \url{https://disconnect.me/disconnect}.
\textsuperscript{270} \url{https://addons.mozilla.org/en-US/firefox/addon/disconnect/?src=search}
\textsuperscript{271} \url{https://chrome.google.com/webstore/detail/disconnect/jeoacafpcbìhiakheiefhpjdfeo}
protect users while they navigate the mobile web. The Disconnect mobile application was designed to work on the same principle as the company’s earlier browser extension, by disintermediating invisible “network calls” between the user’s device and third parties – i.e., websites and services other than the one the user is attempting to connect with.

6.2.1. Differences from desktop

216. But to protect user privacy and security on the mobile platform, Disconnect’s product design had to take account of differences between the desktop and the mobile platforms. On the desktop, users generally get the information and functionality they desire by using a search engine (invariably Google, according to market statistics) to identify the websites most likely to provide what the user is looking for. Users then navigate to the desired sites using a browser (either Google’s Chrome browser or one of its competitors).

217. On the mobile platform, by contrast, consumers can use browsers to navigate to websites, but they generally secure desired information or functionality from mobile applications rather than from mobile websites. According to the market statistics discussed above, Google’s Android operating system is the dominant mobile platform. Consumers on that platform use the Play Store’s search function (or browse function, or Google’s recommendations) to identify and secure (through download from the Play Store) mobile applications appropriate to their needs. Users then launch the applications they have downloaded to get the desired information or functionality.

6.2.2. Coverage

218. As with websites on the desktop, sometimes the mobile applications launched by the user attempt “network calls” to third parties. And sometimes the mobile applications launch advertisements which attempt third party network calls. All such third party network calls create the risk of invisible tracking and exposure to malware, just as on the desktop. So, in order to protect user privacy and security on the mobile platform, Disconnect’s functionality had to cover mobile applications, activity within applications (e.g., ads), and browsing, as well.

219. This broad coverage was particularly important to users on Google’s mobile platform because Google’s rules force users to agree to a blanket request for data before they can use even a single application. Mobile application developers consider the ability to collect data from users to be a key “perk” of developing on the Google platform, as contrasted with the Apple platform where users can decline specific requests for data, one at a time.

6.2.3. VPN innovation

220. Disconnect was the first company to figure out how to block third party tracking globally (i.e., for both browsers and applications) on both the iOS (Apple) and Android (Google) platforms.

---

Disconnect created VPN-based technology to achieve this breakthrough; its invention is patent pending. Disconnect’s VPN-based technology provides some of the benefits of a conventional VPN, but at a fraction of the cost. As explained below, Disconnect passed this cost savings on to its customers. The new technology was principally developed by Disconnect’s Chief Technical Officer Patrick Jackson. Before working for Disconnect, Jackson was employed as a software engineer by the United States National Security Agency (NSA).

221. The new VPN technology required certain modifications in the implementation of the four category lists Disconnect had prepared for its browser extension because the VPN technology could not be employed to permit users to unblock access to sites on an individual basis – each category list had to be blocked or unblocked in its entirety. (Of course, the Disconnect VPN-based products can always be “turned off” by the user after they are installed if the user wishes to reach a site or server on one of the block lists.)

6.2.4. Mobile block list

222. First, Disconnect had to optimize its advertising tracking list for mobile. There are many tracking services that just operate on mobile platforms. So, Disconnect started with the advertising block list it created for its browser extensions, adding mobile trackers that it discovered by analyzing the most popular free mobile applications. Basically, the company’s engineers manually recorded trackers that were detected in the top 100 free applications. Each was analyzed and those that fit the criteria were added to the ad tracker block list.

223. The advertising category list, as optimized for mobile, was blocked in its entirely in the new Disconnect mobile application. The list can be found here: 275 It contains roughly 3000 tracking services and sites. As with the desktop version, it is updated from time to time. And, as with the desktop version, companies have been removed from the list when appropriate.

224. Just as on the desktop, analytics tracking services invisibly follow users around the mobile web and build profiles. But blocking some of the larger analytics tracking services – Google Analytics principally among them – “breaks” (i.e., interferes with the loading of) many webpages, disrupting the user experience. Disconnect blocks all analytics tracking services as the default setting on its browser extensions; the user can unblock any that break important webpages on an individual basis.

225. But since services cannot be unblocked individually on Disconnect products using the VPN-based technology, Disconnect decided to eliminate Google Analytics and a few other analytics services from its block list to avoid disrupting the user experience too much. Disconnect decided to block the remainder of the analytics list.

226. Similarly, although social widgets permit social networking sites to track users, Disconnect’s consumer feedback showed that blocking features such as Facebook Like, +1 or Tweet (in the absence of an unblocking capability that could be used on an case-by-case basis) was undesirable to most users. So, Disconnect left all social widgets unblocked in its mobile

275 https://disconnect.me/lists/malvertising
application. As with analytics, the company, in consultation with its users, tried to balance privacy and security with usability.

227. The content category was left unblocked in Disconnect’s mobile application as well, for the same reasons that the default setting in Disconnect’s browser extension left the content category unblocked; these third party connections provide content for webpages that consumers want.

6.2.5. Malvertising coverage

228. Prompted by increasing concerns over “malvertising” and the attendant risks of identity theft, Disconnect intended its new mobile product to provide users with the most comprehensive protection possible (but consistent with consumers’ desires for useful internet experiences). So, Disconnect added a block list of known or suspected malware sites to the product, along with the list of blocked advertising/analytics trackers, to provide comprehensive protection from “malvertising.” It was not necessary for Disconnect’s browser extensions to contain malware blocking functionality because the leading browsers already contained similar functionality.

229. To be clear on the difference between the two lists, the malware list contains services that are known or suspected purveyors of malware, while the tracker list contains services that invisibly track the user (and sometimes serve ads). Of course, services on the tracker list could be used maliciously to connect users with known or suspected malware sites (i.e., already on the malware block list) or malware sites not yet identified (and therefore not yet on the malware block list). Thus DoubleClick, an advertising tracker, is on the tracker list (and not the malware list) even though it serves malware from time to time, as described elsewhere in this Complaint.

230. In any case, the VPN-based technology of Disconnect’s mobile application requires that all services on both lists be treated the same way. So, Disconnect’s mobile/malvertising app blocks network requests between the services (URLs) on the two lists and the mobile application or site the user is attempting to load, meaning that users cannot visit the domains on either list. This is a bit different than the browser extension which permits users to visit sites on the advertising tracker list, but it does not permit those sites to make a network request to the user when the user is on a different site. (We provide this detail only in the interest of completeness. It is not relevant to the legal and factual issues raised here.)

6.2.6. Malware list

231. Disconnect compiled its malware list by analyzing a number of publicly available malware lists. The company then vetted its list using the Google Safe Browsing API (described above). Google Safe Browsing is an updated list of known or suspected malware sites that Google blocks on the Chrome desktop. Developers can use this list to vet their own applications.

276 E.g., http://malwaredomains.lehigh.edu/files/domains.txt.
277 https://developers.google.com/safe-browsing/
result, the Disconnect list contains about 2000 known or suspected malware sites and is very similar to the Google malware list.

6.2.7. Product name

232. The company called its new mobile product “Disconnect Mobile,” but later changed the name to “Disconnect Malvertising” to avoid confusion with the all-in-one app the company subsequently released. In this Complaint, we usually refer to this mobile product as “Disconnect Malvertising.” But occasionally, for purposes of clarity, we will refer to it as “Disconnect Mobile/Malvertising.” This was the first software product intended to provide comprehensive protection against malvertising.

6.2.8. Product launch

233. The company conducted a “soft launch” of its revolutionary new product on August 20, 2014. A “soft launch” is a common technique in the industry for the live market trial of a new product. Disconnect released its new product to users through the Google Play Store, but without a formal press announcement or a public relations campaign. This permitted the company to assess feedback from real users and make adjustments prior to the product’s formal release.

234. In order to publish the product through the Play Store, Disconnect had to register the application in the Google Play Developer Console and Google had to issue authentication keys so that the application could access APIs. So, although there was no formal product launch, Google was fully informed of the product’s release and cooperated in its publication through the Play Store.

6.2.9. Payment model

235. The soft launch permitted Disconnect to test not only the product’s functionality, but also its user interface, product descriptions, and remuneration strategy. Rather than the “pay-what-you-want” approach that Disconnect had used for its browser extensions, the company decided to employ a “freemium” payment model for its mobile applications. Interested users could download the entire product, but only designated “basic” functionality was made available to users for free.

236. Specifically, Disconnect offered a Basic Privacy Pack that blocks 25 of the largest mobile data collectors from invisibly tracking browsing and in-app activities. A current version of the top 25 list can be found here:278 Under the “freemium” model, if the user likes the product enough to purchase it, he can simply make payment through the Play Store and unlock all the rest of the product’s functionality.

237. As stated in the product description at the time of the soft launch, a user could access the Basic Pack for free and upon payment, two additional packs, one to block malware and the other to block advertising (and analytics) tracking. A screen shot of the product from the Play Store at

278 https://disconnect.me/lists/basicfilter
the time of the soft launch is below:

238. The soft launch was a success. Even without publicity, in only a few days, Google’s records showed that more than 4000 Android users installed the new app. Disconnect had previously soft launched an iOS version of the Mobile/Malvertising app through the Apple Store and that, too, was successful.
By the weekend of August 23, 2014, Apple’s published rankings showed that the Disconnect app had become the top grossing utility application on iTunes:

![Top Grossing iPhone Apps](image)

6.3. Removal by Google

239. But on the afternoon of August 26, 2014, without warning of any kind, Disconnect’s CTO received an email notification from Google that the Mobile/Malvertising app had “been removed from the Google Play Store.” The notification cited, as the reason for the removal, that the app “interferes with … another service or product in an unauthorized manner” in violation of section 4.4 of the Google Developer Distribution Agreement. The notification stated that Disconnect could “revise and upload a policy complaint version” of the application.

240. The Disconnect CTO responded by email the next day (August 27), appealing the removal of the app and asking that the suspension be lifted. (Google’s rules limited the number of characters the appeal could contain.) The CTO’s email stated that Disconnect had exercised particular care not to use any technology that would violate Play Store Guidelines and requested a prompt reply. The entire thread of email correspondence between Disconnect and Google regarding the removal of the malvertising application is contained in Appendix A to this document.

---

279 See [https://play.google.com/about/developer-distribution-agreement.html](https://play.google.com/about/developer-distribution-agreement.html)
6.3.1. Ad blockers

241. When no reply was forthcoming, Disconnect concluded that Google had mistaken the Disconnect product for an “adblocker” and posted an analysis to that effect on its website. In March of 2013, Google had removed several prominent ad-blocking applications from the Play Store, citing section 4.4 of the Developer Agreement. That section prohibits the developer from developing or distributing any product in the Play Store “that interferes with ... the devices, servers, networks, or other properties or services of any third party including ... Android users, Google, or any network operator.”

242. The primary purpose of ad-blocking applications is to improve the browsing experience for users by giving users the option to block or allow ads, rather than to protect user privacy and security. Only a few have separate privacy lists that block third-party tracking requests, and these are not widely used. Of course, in some cases, blocking ads will also block attendant invisible tracking. But for the most part, ad blockers block ads without blocking invisible tracking requests. This is accomplished by blocking the code that formats the display of the ad on the user’s screen, so that the user no longer sees the ad. But the ad, in effect, still “sees” the user.

243. Disconnect’s malvertising app, by contrast, blocks network calls to third party sites/servers/services that engage in invisible, nonconsensual tracking and that distribute malware. If a third party site on the block list tries to use invisible network connections to display an ad, the ad will be blocked. But, as previously explained, not all ads get blocked. Disconnect does not block first party ads, nor ads from servers not on the tracking or malware lists, nor ads from whitelisted servers.

6.3.2. Re-launch

244. With this distinction in mind between blocking ads on one hand, and blocking invisible tracking and malware on the other, Disconnect modified its mobile app, combining the malware and advertising lists into a single “malvertising” pack and rewriting the product description to make clear that invisible trackers and malware, rather than ads, were targeted for blocking. On September 7, 2014, Disconnect resubmitted the revised product (version 2) to the Play Store. Once again, Disconnect registered the application in the Google Play Developer Console, and once again Google cooperated in the publication of the app in the Play Store by issuing authentication codes. On September 8, 2014, Disconnect issued a press release formally

---

280 https://blog.disconnect.me/blog/google-just-banned-our-new-android-app-before-it-even-launched-another-example-of-why-privacy-friendly-alternatives-for-android-app-distribution-are-critically-important


announcing the product. The announcement was picked up by the business and computer press.

245. As with version 1 of the product, users could download the basic pack for free. Because of the efficiency of Disconnect’s VPN-based technology, the company charged only a one-time fee of $10 for unlocking the complete malvertising pack. (By contrast, Disconnect charged an annual fee of $30 for unlimited use of its Secure Wireless app, a somewhat comparable Android app based on a “full-fledged” VPN.) This is a screen shot of version 2 of the Malvertising app available on Google Play, as of September 7, 2014, the date it was formally launched:

6.3.3. Second removal

246. After Disconnect re-implemented its product and registered it once again in the Google Play Developers Console, after Google issued authentication keys and version 2 of the app was published for distribution in the Play Store, after Disconnect issued a press release and


numerous stories were posted about the new product, and after thousands of users (see below) started downloading the product, Google finally got around to responding to the August 27 appeal by the Disconnect CTO of the removal of the first version of the app from the Play Store.

247. In the early evening of September 8, Google sent an email to Disconnect denying the appeal to reinstate the first version of the application, removed from the Play Store two weeks earlier. The first version of the application “interferes with other applications, because it blocks the policy complaint ad serving functionality in third party apps available on the store,” Google wrote. Disconnect’s CEO responded by return email asking for an explanation of the quoted language so that Disconnect could work to ensure compliance.

248. A half hour later Google responded, demanding that Disconnect unpublish the second version of its malvertising application, launched earlier that day. In a subsequent round of email correspondence a couple of hours later, Google claimed that both versions of the malvertising app violated section 4.4 of the Developer Distribution Agreement, quoted above.

249. Shortly after midnight on September 9 (about an hour later), Google informed Disconnect by email that version 2 of the application had been removed from the Play Store, again citing section 4.4 of the Developer Distribution Agreement. Google’s notification ominously threatened even more severe sanctions if Disconnect persisted: “All violations are tracked. Serious or repeated violations of any nature will result in termination of your developer account, and investigation possible termination of related Google accounts.”285 Subsequent requests for guidance from Disconnect were rebuffed by Google.

6.3.4. Consumer response

250. In total, version 2 of Disconnect’s Malvertising app lasted barely 20 hours in the Play Store. But during that short period, more than 20,000 Android users installed the application. 162 of those users rated the application, giving it an average rating of 4.2 stars, all of this according to the data Google provided to Disconnect:

285 See Appendix A.
As of September 9, the Disconnect Mobile/Malvertising application for iOS was the top grossing iPhone utilities application, according to Apple’s statistics:
6.4. Google’s rationale

252. Google claimed to base its action against Disconnect’s Malvertising application on section 4.4 of Google’s Developer Distribution Agreement, which prohibits Disconnect (and any other developer) from distributing any product in the Play Store “that interferes with ... the devices, servers, networks, or other properties or services of any third party including ... Android users, Google, or any network operator.” Google claimed that Disconnect violated section 4.4 because, according to Google, the Malvertising application “interferes with other applications, because it blocks the policy compliant ad serving functionality in third party apps available on the store.”

253. Google’s interpretation and invocation of section 4.4 to justify the removal of Disconnect’s malvertising app unlawfully discriminates against Disconnect in that Google’s conduct is inconsistent with Google’s own stated policies, with Google’s treatment of other, similar Disconnect products, with Google’s treatment of its own less effective privacy and security features, and with Google’s treatment of apps that compete against Disconnect’s Malvertising app.

6.4.1. Inconsistent with Google’s stated policy

254. The Disconnect Malvertising app “interferes with” ad serving functionality only insofar as companies are attempting non-consensually to connect the user to malware sites, to corrupted advertisements, or to sites that invisibly track users and can therefore be used to invade user privacy and to deliver malware, intentionally or otherwise. Ads used for these purposes, collectively known as “malvertising,” could hardly be deemed Google “policy compliant.”

255. Google, though its Safe Browsing technology, warns users to avoid malware sites. Starting in 2009, Google set up a site and developed resources specifically to prevent “malvertising.” And according to Google’s testimony before the U.S. Senate Committee, Google scans and re-scans ads in its system to identify and disable sources of malvertising.

256. Disconnect’s product merely implements what Google says its policy is – to combat malvertising. Google’s own anti-malvertising technologies – warning users about malware sites, teaching publishers how to avoid malvertising, and scanning ads -- “protect” users from sources of malware only after the sources have been identified – by which time millions of users have been exposed. Disconnect’s product disintermediates exposure to invisible tracking sites before they become malicious.

257. In short, the difference between Google’s efforts against malvertising and those of Disconnect is simply that Disconnect’s efforts are effective and Google’s (by design) are not. This is best illustrated by the fact that DoubleClick and AdMob repeatedly have been caught distributing...
malware to users through tainted ads. Indeed, only two weeks after Google removed the Disconnect malvertising app from the Play Store, DoubleClick, presumably unintentionally, served up malicious ads to “millions of computers.” 291 Ten days later, the same thing happened again. 292 And again, even more recently. 293

258. The relatively few Android users who were able to install Disconnect’s malvertising app before its removal from Google’s Play Store were protected from these attacks. Those who were denied easy access to Disconnect’s functionality by Google were not as fortunate.

6.4.2. Inconsistent with prior treatment and interpretation

259. Google’s ban of the malvertising app from the Play Store is not only inconsistent with Google’s stated policy on malvertising. It is also inconsistent with Google’s prior and continuing interpretation of the nearly identical contractual language, under which Google continues to host and distribute Disconnect’s private browsing extension for the Chrome browser (“Disconnect version 2”).

260. Google claimed a violation of section 4.4 of the Play developer agreement, quoted above, as the basis for removing Disconnect’s malvertising app from the Play Store. But virtually identical language governs the distribution of Disconnect’s browser extension from the Chrome Store (prohibiting any product that “interferes with … devices, servers, networks, data, or other properties or services of any third party”) 294. Google continues to host and distribute the extension.

261. Google claimed that the malvertising app violates the section 4.4 language because it “blocks the policy compliant ad serving functionality in third party apps available on the store.” But the Disconnect browser extension that Google continues to distribute from the Chrome Store does the same thing. Neither Disconnect’s private browsing Chrome extension nor Disconnect’s mobile malvertising application block all ads; they both disintermediate calls to sites and services that engage in invisible and potentially malicious tracking, including ad-serving sites that fit the criteria.

262. The malvertising application increases privacy and security coverage by also blocking a list of sites known or suspected to distribute malware, but this malware list is curated using Google’s own malware list and is very similar to Google’s malware list. So, the addition of a malware list provides no basis for Google to treat Disconnect’s mobile malvertising app differently from Disconnect’s browser extension.

263. Both products block ads from servers engaged in invisible tracking, and both therefore “interfere” in the same way with some monetization by third parties. The browser extension

291 http://www.theverge.com/2014/9/19/6537511/google-ad-network-exposed-millions-of-computers-to-malware
294 See Google Chrome Web Store Developer Agreement, section 4.4, https://developer.chrome.com/webstore/terms

64
“interferes” to some extent with the ability of websites to make money by blocking ads on the sites from servers engaged in invisible and potentially malicious tracking. The malvertising app similarly “interferes”—by blocking ads from known tracking services on mobile websites and by blocking the same type of ads on third party mobile applications, since, as explained above, most consumers use mobile apps rather than mobile websites to get information through their phones. The effect of the malvertising app and the browser extension on third party revenues is largely the same.

264. So, the difference in Google’s treatment of the two products cannot be justified by the relevant contractual language or by the operation of the products under that language. But Google’s difference in treatment can certainly be explained by the company’s anticompetitive animus and the market differences in the two situations. Google faces a great deal of competition in the desktop browser market and there are many tracking and ad blocking browser extensions for the desktop. If Google blocked all those extensions, millions upon millions of users would switch to the Safari, Firefox, Opera, and Internet Explorer browsers, none of which would enact a similar ban.

265. By contrast, Google has a monopoly in the mobile operating system market, and there are few good tracking blocker apps for the mobile platform. So, Google can ban Disconnect’s malvertising functionality, knowing that users have nowhere to turn.

6.4.3. Discrimination: Google’s treatment of its own software

266. Google’s removal of Disconnect’s malvertising app from the Play Store unlawfully discriminates against Disconnect in that Google does not apply the prohibition of section 4.4 of the developer agreement or the section’s rationale (as stated by Google) to Google’s own similar but less effective privacy and security functionality. As explained in an earlier section of this Complaint, Google incorporates a number of technical features that it claims protect user privacy and security directly into the dominant Android operating system (or into products or apps that it bundles with the Android operating system, like the Chrome mobile browser). To cite but one example, Google permits users to protect their privacy and security by “opting out” of a certain limited group of “interest-based” ads across the web through a set of menus.295 This feature is bundled into the Android operating system through the “Google Settings/Ads” webpage.296

267. In reality, invoking this feature does little to mitigate privacy and security risks to the user. As explained above, this feature does not prevent Google or other companies from invisibly tracking the user; it only prevents Google from showing the user certain ads. Yet, despite the feature’s limited effectiveness, it most assuredly contravenes section 4.4 of the developer agreement in that it limits third party sites and mobile apps from showing some of the most highly targeted and effective ads, and therefore reduces the revenue that third party sites and apps receive from hosting ads.

295 http://www.google.com/settings/ads?hl=en&sig=ACi0TCFiVoVRK6X3NU1_sbx9RW_UhyFf4iYC30tbi6oq_oXW47mWoc2XisgvmTS4s1PYW7qKbe+PYR2gViokKoiRhBvZv9sH0aXASbbl2b08CJuDow6rhPwFMs5St_PevLudKWM2JWwpp_1bIXWLMd90Uc5s20_Y2VYuAqvHticQr7_fjW26UXuk4wVMl6enN5Rw4
296 See http://www.google.com/ads/preferences/html/mobile-about.html (visit the URL on Android Chrome).
268. So, the bundled Google feature “interferes with” the services of third parties, and specifically, it “interferes with other applications, because it blocks the policy complaint ad serving functionality in third party apps available on the [Play] store” -- precisely the rationale Google gave for removing the Disconnect Malvertising application. (Of course, neither the Google bundled feature nor the Disconnect app block all ads.)

269. Google has used its dominant mobile operating system position to make Disconnect’s superior privacy and security functionality well-nigh unavailable to Android users based on a rationale that, if applied consistently, would also require the removal of Google’s less effective privacy and security functionality. But Google has not applied its rules consistently. Rather, Google has used its dominant mobile operating system position to insinuate its own less effective technology into the market, to the detriment of both its rival Disconnect and its own users.

6.4.4. Discrimination: Treatment of Disconnect’s competitors

270. Google’s conduct is discriminatory for a second reason as well. Google has used its dominant operating system position to make Disconnect’s app virtually unavailable to Android users, citing a rationale (section 4.4) that if applied consistently would also require the removal from the Play Store of applications that compete with Disconnect’s malvertising app. But instead, Google has permitted these competitors’ less effective privacy and security apps to remain in the Play Store. And Google has bundled the Play Store with its dominant mobile operating system in its agreements with handset makers, meaning that Google has used its dominant position to insinuate the inferior products of Disconnect’s competitors into the market, to the detriment of Disconnect and Android users.

271. For example, for several years, a company originally called Evidon and now called Ghostery has published and distributed through the Chrome Store a browser extension that identifies and blocks invisible tracking from certain designated third party services.297 In other words, Ghostery’s browser extension (available through the Chrome Store) does the same thing that Disconnect’s private browsing extension does.

272. While the two companies’ products are quite similar, their business plans could not be more different. Ghostery is basically an ad tech company masquerading as a privacy company. The company has been severely criticized by privacy advocates for selling the data it collects from its own users, albeit not always with clear disclosure.298 One of its customers is credit score company Equifax; another is Proctor & Gamble, the consumer products company.299 As one journalist explained, “Ghostery blocks sites from gathering personal information on you – but [a service of its parent company] will take note of the ads you encounter and those you block, and sells that information to advertisers so they can better formulate their ads to avoid being blocked.”300

297 https://chrome.google.com/webstore/detail/ghostery/mlomiejdklochcfejiclbmpeanij
298 See, e.g., http://www.technologyreview.com/news/516156/a-popular-ad-blocker-also-helps-the-ad-industry/
273. Google has partnered with Ghostery’s parent company in an advertising industry initiative that has been criticized by EU policymakers as an effort that confuses users and discourages adoption of the far more protective Do Not Track initiative.\(^{301}\)

274. In late 2014, Ghostery released a mobile browser for publication and distribution through the Google Play Store. According to the product description in the Play Store, the “Ghostery Privacy Browser” has the functionality of the Ghostery browser plugin “built in,” and it similarly collects and sells user information.\(^{302}\) As one journalist observed, “Ghostery, the new Android ‘privacy browser,’ is ultimately no different from Google’s Chrome in that you – your data – are its product, not its primary customer.”\(^{303}\)

275. The Ghostery mobile browser most assuredly “interferes” with monetization by third party mobile websites, in that the browser blocks tracking and site publishers, therefore, cannot charge tracking services as much for hosting and enabling their invisible tracking. Nevertheless, while the Disconnect malvertising application (that blocks tracking) has been removed from the Play Store, the Ghostery browser (that also blocks tracking) not only remains there, but can easily be found by a consumer using the Play Store’s search function. The Ghostery browser appears, for example, in the top row of responses to a user query for “privacy” applications:

---


\(^{303}\) [https://gigaom.com/2014/12/03/ad-tech-firm-ghostery-releases-a-privacy-focused-android-browser/](https://gigaom.com/2014/12/03/ad-tech-firm-ghostery-releases-a-privacy-focused-android-browser/)
276. Of course, mobile users invariably invoke mobile applications (rather than browsing) to find content and services on the mobile web. Browsing on a small mobile device is cumbersome and, hence, little used. And Ghostery’s browser does not protect against tracking by mobile applications, in-app activities, or ads launched by mobile applications, at all. Therefore, it not a realistic source of privacy protection for mobile users. Doubtless for that reason, as well as Ghostery’s collection and sale of user information, Google has permitted the Ghostery browser to stay in the Play Store, while discriminating against Disconnect.

277. Ghostery has also released a second mobile product that Google publishes and distributes through the Play Store – Ad Control. This Ghostery mobile application permits mobile users to “opt out of receiving personalized ads” from a specified group of companies. Ad Control covers ads launched by other mobile applications.304

278. Like the Google feature bundled into the Android operating system that permits users to “opt out” of interest-based ads, the Ad Control app does not prevent invisible tracking at all. It merely prevents website publishers and advertisers from showing “personalized ads” – not even all ads. Nevertheless, the Ad Control app contravenes section 4.4 of the developer agreement in that it limits third party mobile apps from showing some of the most highly targeted and effective ads, and therefore reduces the revenue that third party apps receive from hosting ads. So, Ad Control “interferes with” the services of third party apps and, more specifically blocks policy compliant third party ad serving functionality – the rationale Google gave for removing Disconnect’s malvertising app from the Play Store.

279. Google’s policies and practices discriminate against Disconnect and favor both Google’s own ineffective privacy and security features and the ineffective privacy and security features of mobile applications that compete with Disconnect’s far better products. Google’s conduct improperly restricts consumer choice and retards investment and innovation in personal privacy and security solutions. Google engages in these practices so as to confuse and mislead consumers into accepting ineffective privacy and security solutions, with the aim of maintaining and increasing its revenues from highly targeted advertising, to the detriment of both consumers and its market rival Disconnect.

6.5. All-in-One (AiO) application

280. On November 13, 2014, Disconnect released a new generation product that combines all the functionality the company had created for previous products including private browsing (blocks invisible connections to more than 5000 tracking and malware sites and services), “Smart VPN” technology (encrypts all user internet connections and masks the user’s location),

private/anonymous search (strips personally identifying information from search queries), and visualization (of undisclosed web tracking and privacy policies) technology.  

281. In visualization mode, the new product identifies invisible mobile tracking sites seeking to connect with the user’s device and tallies the number of unsecured connections the tracking requests have created. (This is depicted on the cover of this Complaint.) Unsecured connections permit “man-in-the-middle” attacks including “sidejacking,” in which malicious actors “snoop on” network traffic and intercept user passwords, account information and the like.  

282. When the protection mode is invoked, the Disconnect product encrypts all internet connections and blocks invisible network connections with sites and servers on the company’s malvertising list (advertising trackers, analytics trackers and known or suspected malware sites), including in-app activity on mobile devices. The Disconnect product even blocks so-called “supercookies” – code that telecommunication carriers increasingly add to HTTP requests to make it easier for advertisers to track them.  

283. The new product runs as a stand-alone application on the major desktop (Windows and Mac) and mobile (Android and iOS) platforms. It is available for download from the Disconnect site and the Apple Store. However, Disconnect did not submit the new application for publication in the Play Store because the new all-in-one application uses the same malvertising block list (advertising trackers, analytics trackers and malware sites) as the earlier mobile malvertising application for the Android platform, which Google twice removed from the Play Store.  

284. As explained above, when Google notified Disconnect that the malvertising application had been removed from the Play Store, Google warned that “repeated violations of any nature will result in termination of your developer account.”  

285. Although Disconnect’s malvertising application for the Android platform has been removed from the Play Store, it remains available for download from the Disconnect site. However, as explained below, user difficulties in installing the app from a source other than the Play Store (known as “sideloading”), along with other impediments created by Google, have all but killed the market for the product.  

---

305. [Link to PR Newswire]
306. [Link to Tom's Guide]
307. [Link to Ars Technica]
308. [Link to Gigacom]
309. See Appendix B.
310. [Link to Disconnect website]
286. Separately, when Apple released an updated version of its operating system, it produced certain incompatibilities with the malvertising product. Disconnect decided to withdraw the malvertising app from the Apple Store rather than rework it, preferring to use the resources on the new all-in-one app, which contains the same private browsing functionality, along with many other privacy and security features. The all-in-one app remains available for download from the Apple Store.³¹¹

³¹¹ https://itunes.apple.com/app/id935480186
7. **Anticompetitive Effects of Removal**

7.1. **Introduction**

287. When Google removed Disconnect’s malvertising app from the Play Store, Google sought to explain away the anticompetitive effects of its exclusionary conduct by cynically suggesting that users could simply download the banned app from the Disconnect site and install it on their Android devices themselves – a process known as “sideloading.”

Following Google’s lead, the press has suggested, perhaps unintentionally, that exclusion from the Play Store amounts to little more than “removing easy access” to a banned app and decreasing its “visibility to the mainstream Android user” – impediments that can be addressed to some extent with “alternative methods” of distribution, namely sideloading.

288. In fact, while users (as explained below) may find desirable apps easily on the Play Store and install them effortlessly with a couple of clicks, the vast majority of Android users have likely never sideloaded an app and may not even be aware that apps can be secured from developer websites, if they are not on the Play Store. Most assuredly, users are not familiar with the cumbersome, difficult, confusing and potentially dangerous procedures for sideloading on an Android device. The uncertainty of these procedures constitutes an enormous barrier to market for Disconnect’s banned apps. We illustrate this below.

289. More importantly, focusing only the difficult installation procedure Google has imposed on Disconnect users ignores even greater anticompetitive effects of Google’s ban. Google’s actions against Disconnect’s malvertising technology have all but eliminated the ability of Android users to find and evaluate Disconnect’s malvertising and AiO apps in the first place. And Google’s removal of the malvertising app from the Play Store has denied Disconnect key functionality need to upgrade and improve its malvertising and AiO apps going forward. These effects have greatly reduced the sales of Disconnect’s malvertising and AiO apps, as we demonstrate below, and continue to irreparably injure the future prospects for Disconnect’s products.

7.2. **Loss of distribution / marketing / identification**

290. When Google removed the malvertising app from the Play Store, Disconnect lost the only effective mobile distribution platform for its malvertising technology. Google controls the dominant mobile platform (Android) in Europe and worldwide. The Play Store, the only aggregation facility through which Android users can seamlessly secure mobile apps, comes bundled with Android in contracts with handset makers. By these contracts, the handset makers must prominently display access to the Play Store.

291. Google has collected almost 1.5 million applications into the Play Store, making the Store a “one-stop” destination for all of a user’s Android application needs. According to Google, “Google Play is the premier store for distributing Android apps,” “a central part of the Android

---


313 See, e.g., [http://techcrunch.com/2013/03/14/adblock-plusresponds-to-google-play-bar/](http://techcrunch.com/2013/03/14/adblock-plusresponds-to-google-play-bar/); [http://techcrunch.com/2013/03/13/google-pulls-ad-blocking-apps-from-play-store-for-violating-developer-distribution-agreement/](http://techcrunch.com/2013/03/13/google-pulls-ad-blocking-apps-from-play-store-for-violating-developer-distribution-agreement/)
experience,” and “a top destination for web users.” Google touts the Play Store to developers as an essential mechanism to reach Android users: “Google Play now reaches more than 1 billion people on Android devices in more than 190 countries, helping a growing number of developers like you build successful global businesses.”

7.3. Loss of placement in search results

292. With such a vast number of available Android applications, users need a mechanism by which to locate and identify the apps they desire. And developers need a “discovery” mechanism by which they can reach interested users. Just as with conventional websites, being “found” by users vital to developers. According to Google, “[a]pp discovery plays a critical role in driving” developer success. As the Google executive in charge of the Play Store recently explained, “[u]ser are trying to discover apps, and we are trying to improve the app discovery process, and developers are trying to reach users.”

7.3.1. “Organic” search results

293. Google provides a keyword search mechanism in the Play Store by which a user can locate and identify (with a particular functionality) desirable apps. The Play Store search mechanism works much the same way as Google’s familiar organic search functionality for web information and services. According to Google, “[s]earch uses powerful heuristics to suggest terms as the user types [a query for an app], and it offers direct links to apps as suggestions.” Play Store search results are listed with “the most relevant, most popular apps at the top,” similar to organic listings in desktop search.

294. This is how simple it is to find Disconnect’s Secure Wireless mobile app in the Play Store using the search function:

314 http://developer.android.com/distribute/googleplay/about.html
315 http://android-developers.blogspot.com/2015/02/a-new-way-to-promote-your-app-on-google.html
316 http://android-developers.blogspot.com/2015/02/a-new-way-to-promote-your-app-on-google.html
318 http://developer.android.com/distribute/googleplay/about.html
7.3.2. “Paid” search

295. And, as with Google’s familiar desktop horizontal (or general) search results, developers can buy search ads to increase the likelihood that users will find their products. As Google has explained, “[s]earch ads on Google Play will enable developers to drive more awareness of their apps and provide consumers new ways to discover apps that they might otherwise have missed.”

296. Indeed, Google simply copied the search/search advertising model that it has employed for horizontal search and applied it to mobile apps in the Play Store, as the Google executive in charge of Play recently admitted: “Users [of horizontal search] are looking for information, we provide them with organic information, but at the same time we allow companies to use sponsored ads to reach users too. We think the same model works very well for Play.”

297. To continue the analogy or “model” that Google itself uses to describe Play Store search functionality, Google now stands accused by the European Commission of abusing its dominance by penalizing (demoting) its specialty search rivals in its general search results. Demoted specialty search rivals, according to the Commission’s documents, have lost user traffic they would otherwise have received. By comparison, Google’s unlawful sanction against its privacy and security rival Disconnect is even more severe. Disconnect’s malvertising and AiO applications are not included in the Play Store search results (even in search ads) at all; Disconnect’s malvertising apps get no traffic -- not simply diminished traffic -- from Google’s dominant platform as a result of Google’s exclusionary practices.

319 http://android-developers.blogspot.com/2015/02/a-new-way-to-promote-your-app-on-google.html
7.4. Loss of other placement

298. Loss of placement in browsing and other results: Google’s Play Store includes other mechanisms, beyond search and search advertising, through which a developer can enable users to find his applications. When a developer publishes an app in the Play Store, for example, the developer places the app in one of roughly 30 categories. Users may browse the categories looking for desirable apps. As with Play Store app search results, apps in each category are listed for the user based on user ratings, reviews, and downloads, among other criteria. 321

299. Similarly, Google publishes, both daily and weekly, a number of curated lists of Android apps for promotion to users in the Play Store – i.e., to bring specific apps “to the attention of users.” These promotions “have driven hundreds of millions of app downloads” to the obvious benefit of favored developers. 322

7.5. Loss of ability to be found

300. When Google removed the malvertising app from the Play Store, Disconnect lost the ability to have its malvertising and AiO apps “found” by users through the Play Store search and browse features and from Google’s many curated promotional lists. Of course, an app developer whose product is banned from the Play Store might try other mechanisms for bringing his app to the attention of consumers – placement in other app stores, press releases, word of mouth, etc. And perhaps a developer might even count on being listed in the desktop or mobile horizontal search results (rather than the Play Store search results) to garner user attention.

301. But none of these other techniques, individually or combined, constitute an adequate or even remotely plausible substitute for inclusion in the Play Store, with its attendant “discovery” and promotion features. Consumers invariably use the Play Store features, particularly search, to find desirable apps. According to Google, “for the average app, search makes up the vast majority of installs.” An independent study found that “75% of users found apps on Google Play through a search.” 324

302. Other techniques fail to generate suffice user interest to sustain market participation, as Disconnect’s financial results, discussed below, demonstrate. For all intents and purposes, removal from the Play Store put the entirety of the Android market, roughly 80% of all mobile devices, off limits to Disconnect’s private browsing applications.

7.6. Loss of association with high quality

303. Even if Disconnect’s malvertising and AiO applications came to the attention of some users after removal from the Play Store (though an article in the computer press, for example),

321 http://developer.android.com/distribute/googleplay/about.html
322 http://developer.android.com/distribute/googleplay/about.html
324 http://www.adweek.com/socialtimes/google-discloses-how-search-for-google-play-works-for-the-first-time-12-percent-of-dau-search-for-apps-daily/539639
325 http://www.fiksu.com/assets/ebooks/android-app-marketing-and-google-play.pdf
exclusion from the Play Store denied the Disconnect apps the credibility and association with high quality that inclusion in the Play Store conveys – making it unlikely that consumers would even try to download the apps from an alternative source. For example, at the time Google removed the malvertising app from the Play Store, it had a 4.4 star (user) rating. This record was removed with the app and became unavailable to potential purchasers. As the Google site explains, “[p]rospective users look at ratings and reviews as key benchmarks of app quality.”326

304. Most assuredly, Disconnect could have posted user ratings on its own site. But they would not have conveyed the objectivity and credibility or the imprimatur of excellence that good reviews on the Play Store site convey.

7.7. Loss of easy downloading

305. Android apps that are included in the Play Store can be downloaded and installed on the user’s Android phone quickly and easily – with literally two clicks and no confusion. Google has not removed Disconnect’s Secure Wireless app from the Play Store, and, hence, that app can be downloaded easily from the Store. When the user locates the app by using the Play Store browse feature, or by typing the app name or keyword description into the search bar, or from any of Google’s curated lists, the user selects the Disconnect app and taps “install”:

---

326 http://developer.android.com/distribute/googleplay/about.html
Then the user taps “accept” to allow the app to use the device’s Wi-Fi connection (or to purchase the premium version) and downloading begins:

The downloading and installation is competed automatically, without user involvement:
7.7.1. Fragmentation Issues

306. Google takes the position that “sideloading” the banned apps from the Disconnect site is equally straightforward. But, if an Android user even learns about the banned Disconnect apps, and knows enough to go to the Disconnect site to try and install them on his Android device, he faces a daunting process, which we simplify for purposes of discussion below. Much of the difficulty and confusion in the sideloading process (and much of Disconnect’s broader difficulties in supporting users and maintaining the integrity of its malvertising and AiO applications following the removal from the Play Store – as we explain below) stems from the fragmentation that still characterizes the Android platform.

307. Google has released many versions of the Android operating system. Six of these differing versions are still in widespread use on large numbers of mobile devices.\(^{327}\) Differences in the “skin” of various manufacturers – i.e., differences in packaging and external interfaces – further exacerbate the fragmentation of the Android platform produced by the different OS versions. As explained above, Google has increasingly taken services, functions and interfaces (APIs) out of the operating system and put them into one of the centralizing facilities associated with the Play Store.\(^{328}\)

308. Without access to these centralizing facilities, including APIs, Android app developers bear an enormous burden in that, to gain access to the lion’s share of the market, they must develop and support the same applications across a myriad of very different platforms, all named “Android.” This is well beyond the capabilities and resources of all but the very largest Google competitors, and even they would likely run at a loss trying to execute such a business plan.\(^{329}\) It is well beyond the capabilities and resources of young, entrepreneurial companies attempting to challenge Google.

309. Google makes the Google Play Developers Console and certain other key centralizing functionality available to developers only through the Play Store. So, when Google removed the malvertising application from the Play Store, Disconnect lost access to certain key centralizing functionality for its malvertising and AiO apps that we describe in some detail below.

7.7.2. Sideloading procedure

310. Among the centralizing features that Google provides for the developers in the Play Store is the simple download and installation mechanism illustrated above, by which users can easily download and install Android apps from the Play Store with little concern over the specific manufacturer’s device or version of Android it is operating. Without this simple download and installation mechanism for its malvertising technology, the burdens of fragmentation effectively preclude success for Disconnect’s malvertising and AiO mobile apps. And Google further burdens the sideloading process for Disconnect’s prospective customers by posting a sequence

\(^{327}\) http://developer.android.com/about/dashboards/index.html

\(^{328}\) http://www.androidcentral.com/new-google-play-services

\(^{329}\) See http://www.forbes.com/sites/ewanspence/2014/06/25/google-has-93-of-android-users-on-the-latest-google-play-service-outperforming-apples-ios7-adoption-rate/
of misleadingly menacing warning screens at various junctures in the process which are intended to dissuade users from sideloading the Disconnect apps.

311. The sideloading process varies widely from device to device, depending on the Android version the user has, the manufacturer’s “skin,” and the type of mobile browser the user is navigating with, producing a staggering number of permutations. We summarize them into a few steps below. First, if an Android user learns of and wants the Disconnect malvertising or AiO app, he must first know enough to navigate to the Disconnect site using his mobile browser in order to get them. But when he tries to download the apps onto his Android phone from the Disconnect site, he will get the following message from Google:

7.7.3. Menu variations

312. To continue with the installation, the user next has to know that he needs to invoke the “unknown sources” option in his phones menus. Google does not tell him this. Moreover, the location in the menus of the “unknown sources” option varies from device to device, based on the manufacturer. For the HTC Droid Incredible, for example, the user must navigate to the “settings” menu, and then to the “applications” menu to find the “unknown sources” option:
For the Motorola Moto G, on the other hand, the user must navigate from the “settings” menu to the “security” menu in order to find the “unknown sources” option:

These are only a couple of examples of the initial menu variations Android users encounter in trying to sideload. The “settings” menu is frequently customized by the device manufacturers.
7.7.4. Menacing warnings

313. Once the user finds and invokes the “unknown sources” option, he will receive a menacing security warning from Google. Here are three examples from Europe:

The warning in English says: “Attention! Your phone and personal data are more vulnerable to attack by applications from unknown sources. You agree that you are solely responsible for any damage to your phone or loss of data that may result from using these applications.”

314. Of course, Google knows full well that the Disconnect’s apps are not a source of security concerns. Google accepted the malvertising app into the Play Store twice, and removed the app only because it blocked network requests from invisible, unsolicited tracking services and malware sites – not for any security issues. Nevertheless, Google posts these menacing security warnings in an obvious attempt to intimidate and dissuade the user.

315. As explained above in considerable detail, Google’s Play Store, through the distribution of tainted mobile applications, is a persistent source of malware dangers to consumers. In none of those cases of malware distribution did Google give its Play Store users any security warnings in advance. Google simply permitted the download of tainted apps through its normal two-click procedure. Yet Google gives users the most menacing security warnings when they try to sideload Disconnect apps, despite Google knowing full well that Disconnect’s apps constitute no security risk to users.

7.7.5. Continuing security risk

316. In any event, if the user either continues the sideloading process to completion or gives up because of Google’s misleading threats after checking the “unknown sources” option, Android does not prompt the user to “uncheck” the “unknown sources” option. That option remains
open and, depending on the mobile browser the user is navigating with, the user may thereafter sideload an app that is truly dangerous without being warned at all about the security risk. In other words, Google convoluted and menacing sideloading procedure actually increases rather than mitigates the security risk to the user.

7.7.6. Additional menacing warnings

317. To continue the sideloading procedure, the user must know enough about Disconnect (and Google) to ignore the menacing warnings and click “ok” or the equivalent. The user may then proceed to download the Disconnect application package (known as an “APK,” or “Android Application Package”) from the Disconnect site to his phone. But if the user is using Google’s Chrome browser, he will frequently get yet another menacing security warning. This is what appears on the user’s screen on the Samsung Galaxy S5 with the Chrome browser:

A user on the same devise navigating with the Firefox browser does not get this warning. Only Google sees the need to repeatedly frighten users wishing to sideload Disconnect apps.
7.7.7. Locating the APK

If the user clicks “ok” (or does not receive the warning), he can complete the download. But once the file is downloaded from the Disconnect site, the user must locate the APK among the various files in his local file directory in order to open and install it. Many users will need to find, download and install an additional file manager application just to browse local files to find the APK.  

7.7.8. Additional warnings

Frequently, after locating the downloaded APK, the user must ignore yet another security warning in order to open the file. Moreover, the process of opening the downloaded APK differs depending on the third party software resident on the user’s device. For example, the Galaxy Mini presents the user with a dialog box not found on other devices:

320. After locating the APK, clicking through the various warning and dialog boxes, and opening the APK, the user may click to install it on his device. Given the daunting nature of the sideloading process on Android, it is small wonder that so few users successfully complete it – as the financial data below demonstrates.

7.8. Loss of GPDC functions

When Google removed the malvertising app from the Play Store and threatened further action against other Disconnect apps that provide malvertising protection, Disconnect lost the ability to register those apps (malvertising and All-in-One) through the Google Play Developer Console,  

one of the centralizing facilities for features, services, functionality and APIs described above. So, in addition to losing the ability to have these apps promoted, found, downloaded and installed by users through the dominant Play Store platform, Disconnect also lost access to key features, functionality and services for these apps provided through the GPDC. Some of the key functions are described on Google’s Developer Console page. Disconnect also lost access to several key APIs for these apps.

322. Some of the lost GPDC functions (including Upload and Instantly Install, Capabilities Targeting, Multiple APK Support, and Crash Reports) and lost APIs (Billing) had both an immediate and long-term effect on the customer acceptance and market viability of Disconnect’s banned products. We summarize those effects below. It is worth noting, for purposes of comparison, that Google’s abuse of desktop search dominance did not include damaging the utility of competitors’ products by denying them key functionality – precisely what Google has done here.

7.9. Loss of Upload / Install

323. Google provides “Upload and Instantly Install” functionality for the apps in the Play Store, giving developers the ability to upload the latest Android Application Package (APK) (i.e., the latest version of the developer’s app) to the Play Store and have Google automatically update all users to the latest version of the app. Users of apps in the Play Store, then, can automatically update their apps (in the background, whether the particular app is opened or not) as soon as a new version is available (this is the default setting), or get notification inside their devices that an update is available (again whether the app is opened or not) and manually update the app.

324. Once the Malvertising app was banned from the Play Store, Android users had to re-install the relevant APK in order to update theDisconnect malvertising and AiO apps. Automatic updating was not available. In fact, Disconnect lost the ability even to notify existing users of the malvertising app inside their devices that an update was available. So, Disconnect told users that they had to check back to the Disconnect site from time to time to see if updates were available. And as the company produced updates, they were posted on the site for loading by the user.

325. This situation was unsatisfactory for Disconnect and dangerous for the user. Disconnect lost the ability to easily maximize customer satisfaction and company revenues by upgrading users to the newest version of its product. More importantly, the company could not force an upgrade even if its product was found to contain a critical security flaw. It could not even alert users that a security patch was available.

326. So, the company decided that it had to build the ability to update users on its own. This required the company, first, to build a server side “endpoint” that always made the latest APK available. Then the company’s developers had to write code in each of the banned APKs so that

---

a user’s device would check back to the Disconnect server’s “endpoint” to ensure that the latest version of the product was being run.

327. This undertaking required Disconnect to take developers off of crucial existing projects in order to try and replicate functionality that Google had previously provided. The effort took two weeks of developer time and stretched over three weeks of elapsed time (from roughly August 26, 2014, when Disconnect’s app was first banned by Google, through September 17, 2014, when the updating capability “went live”).

328. Despite the investment of time and resources, Disconnect could not fully replicate Google’s functionality. As a result, even with all the work, the function of checking back to the server can only be initiated by the Disconnect code when the user opens the Disconnect app. When the user opens the app, Disconnect displays an update notification if the user’s app is not up to date, and the user can then manually click to download the latest version of the APK with the application. So, Disconnect still cannot force an update even for a critical security issue.

7.10. Loss of Multiple APK Support

329. One of the various ways Google has addressed the fragmentation issue is to provide “Multiple APK Support” for applications in the Play Store. This allows the developer to seamlessly distribute different APKs to different devices, permitting the developer easily to fix bugs or add features related to specific devices or specific versions of Android.333

330. Disconnect lost this benefit for the Malvertising app when it was banned from the Play Store and cannot provide a comparable substitute. The Android versions of the malvertising and all-in-one apps now require side loading, a confusing and difficult process for the user. Trying to implement multiple APK support would further complicate the install flow and would require Disconnect to rely on the user to identify his or her specific device hardware for support.

331. So, Disconnect does not have multiple APK support for its Android applications that are not in the Play Store. Rather, Disconnect publishes its principal APK, and if a user’s hardware is not compatible, Disconnect has to tell the user that the company does not support the device platform. At bottom, Google’s withdrawal of multiple APK support has effectively denied many Android users the ability to run Disconnect’s malvertising functionality.

7.11. Loss of Capabilities Targeting

332. Another benefit provided by Google for applications in the Play Store is “capabilities targeting.”334 This functionality lets developers know which device models are not supported for their app, based on an analysis of their application’s dependencies, and permits them to limit distribution of their applications to compatible devices. So, users do not experience the frustration of downloading applications that do not work with their devices.

333. Disconnect no longer receives this “capabilities targeting” functionality with regard to the malvertising or AiO application. The company cannot feasibly duplicate this function. Hence, Disconnect has no way to know whether a particular user’s device is compatible with its malvertising and AiO software until the user actually downloads it. The user has to download the software to see if it works – with the attendant (and unnecessary) frustration and ill will.

7.12. Loss of Crash Reports

334. Google also provides an extremely easy way for users to submit “crash reports” (one button whenever the app crashes) for apps in the Play Store. Crash reports facilitate application debugging and improvement. They provide the developer with all kinds of detailed information about the crash, including “stack trace,” device hardware, operating system version and application version, so that the problem can be identified precisely, isolated and corrected quickly.

335. When the malvertising app was banned from the Play Store, Google stopped supplying crash reports on that product. Disconnect lacks the expertise, the time and the resources to implement its own crash reporting system. So, it now has to rely on users emailing the company when they experience a problem with one of the apps that provides malvertising and private browsing protection. Few users are likely to do so, and even those who do would not know to provide the detailed type of information that Google routinely includes. Hence, Google’s withdrawal of information will continue to impede Disconnect’s development efforts for the foreseeable future.

7.13. Loss of Billing API

336. Loss of Google Play Billing API. When the malvertising app was banned from Google Play, Disconnect lost access to the Google Play Billing API for the malvertising application, and Google would no longer accept process payment for that app through its automated system in the Play Store. As explained below, this change occurred after thousands of users had downloaded the free, “Basic” version of Disconnect’s product and before they tried to upgrade to the Premium version by making payment. As previously explained, the All-in-One app for Android has not been tendered to the Play Store, so Google won’t process payment for that app either.

337. Generally, a user on Google Play registers a form of payment (e.g., a credit card or direct carrier billing) for paid app downloads, in-app purchases and subscriptions. Google Play then handles all check out details so that the application developers never have to directly process any financial transactions. Once a consumer completes one transaction in Google Play, he or she can then buy additional apps, music, movies and books without the inconvenience of re-entering credit and financial information.

336 https://support.google.com/googleplay/answer/2651410?hl=en
337 http://www.androidpit.com/buy-paid-app-google-play
338. The consumer’s ability to interact directly with Google (rather than with a small, unknown application developer), along with network effects and economies of scale, make it far easier for developers to overcome consumer reluctance to purchase new applications because of administrative, security, and privacy considerations by using Google Play’s transaction processing. This is particularly true with respect to the “freemium” model of app distribution (used by Disconnect) in which the consumer downloads a more basic free version of the application with limited features and then upgrades to a version with far greater functionality by paying a fee.338

339. By way of illustration, the screen shot sequence below shows the simple procedure by which a user can upgrade to the premium version of Disconnect’s Secure Wireless app, which is still in the Play Store:

340. But as a result of Google’s ban, this desirable approach of using the Google Play Billing API was no longer available to Disconnect for its malvertising and AiO apps. Disconnect still needed to make money, of course, so it built out and contracted for a payment processing firm to take credit card information on Disconnect’s site.  

341. This provided Disconnect with a payment mechanism, but it did not address user concerns about administrative inconvenience and security. Using this third party approach, Disconnect was asking consumers, after downloading the free versions of Disconnect’s apps, to enter confidential credit card information on a small developer’s site (rather than Google’s site) for very small financial transactions -- $5, for example, for a month’s use of the malvertising application – in order to upgrade to the premium version. Despite the interest in Disconnect’s products, these issues proved to be enormous impediments to sales.

342. Google’s withdrawal of the Billing API killed the market introduction of the malvertising product. The publicity attendant to the soft launch and formal re-launch of the malvertising product created enormous consumer interest in the product, and many thousands of users downloaded the “basic” (free) version from the Play Store to try the product. But when they were subsequently interested in upgrading to the premium version of the product, the Google Play transaction processing was no longer available because of Google’s removal of the app from the Play Store. So, prospective purchasers had to enter credit card information for small amounts from the developer’s site – something that they were reluctant to do. Of the many thousands of users who downloaded the Basic version of the malvertising app at the product’s introduction, Disconnect was able to convert very few into paying customers.


343. Without access to the Play Store platform for promotion, distribution, getting “found,” easy downloading, and the like, and without the functionality provided by Google through the GPDC and the related APIs, downloads of the malvertising app plummeted – notwithstanding all of the user interest. [ --------------------- CONFIDENTIAL ---------------------].

344. Disconnect’s all-in-one product was introduced with great fanfare and has flourished on the Windows, Mac, and iOS platforms. It is available for easy download for iOS devices through the Apple Store but the Android version (as a result of Google’s ban) must be sideloaded from the Disconnect site. Nothing demonstrates the anticompetitive consequences of Google’s withdrawal of the Play Store platform and the attendant GPDC technology and related APIs as well as comparing the financial performance of iOS and Android versions of the all-in-one product.

345. [ --------------------- CONFIDENTIAL ---------------------]

339 https://stripe.com/
7.15. Loss of other APIs

346. There are a number of Application Programmer Interfaces (APIs) that Play application developers must “call” within the developers’ code to incorporate key Google functionality and interoperability. In addition to the Billing API, Disconnect lost access to at least three other APIs as a result of Google’s action: Cloud Messaging, App Indexing, and Licensing.

347. The other APIs to which Disconnect lost access did not immediately impact the malvertising and AiO apps, but their unavailability will diminish the functional capabilities of future versions of Disconnect’s malvertising products. The API for Google Cloud Messaging, for example, makes it easier and more resource efficient to communicate between an application and Google servers. So, Disconnect’s development of an encrypted chat capability, for example, will be far more difficult and of lower quality.

348. The Google App Indexing API permits a developer to set up a link between server URLs in Google Search and pages to open in an app. Without that API (now denied by Google to the malvertising apps), Disconnect’s ability to build informational features like a privacy wiki that permits users to search and open results from in-app content using Google Search is substantially diminished.

349. And finally, the Google Play Licensing API is used to control app distribution and prevent piracy. Without that API (now denied) it is far more difficult for Disconnect to limit piracy if it implements a paygate or some other form of upfront billing. These APIs, now denied to Disconnects malvertising and AiO apps, dramatically limit the company’s ability to innovate.

350. As of this writing, Disconnect can still secure access for the malvertising and AiO apps to APIs that are managed by Google through a different developer console (not the Google Play Developer Console), meaning that services such as Google+, YouTube, and Google Drive continue to be available. But one would logically assume that Google will in the future consolidate API access through the GPDC, making all the APIs unavailable to applications banned from the Play Store.

351. Even in the interim, Google could easily further discipline Disconnect by revoking its authorization to the remaining permitted APIs for applications that provide malvertising protection, and, more harshly, by revoking access to APIs for other Disconnect applications. In Google’s email correspondence with Disconnect over the banning of the malvertising app (email of August 28, 2014), Google threatened Disconnect with termination of its developer account for “additional violations in this [app] or additional apps on the [Play] store.” Termination of the developer account would deny Disconnect access to all APIs that require registration and authentication through any Google developer console, including all of those discussed above (those currently managed through the GPDC and otherwise), for all of its applications.
8. LEGAL ARGUMENTS AND REMEDY PROPOSALS

8.1. Markets

352. The markets for mobile operating systems, mobile application “stores,” and mobile browsers constitute distinct and cognizable antitrust markets. These markets are characterized by network effects, economies of scale, and high barriers to entry.

353. Google has a dominant position in each of these markets, evidenced by its high market share and other factors, as explained in this Complaint. Google’s actions in these markets are largely insensitive to the actions and reactions of competitors, customers, and consumers.

354. The market for mobile privacy and security software constitutes a distinct and cognizable antitrust market. This is evidenced by the plethora of mobile privacy and security software, the consumer demand for Disconnect’s malvertising product in the Play Store and Apple Store, as well as other factors set forth in this Complaint.

355. Through various patterns of conduct, Google has abused its market dominance in contravention of Article 102 TEU, by among other actions, illegal tying, discontinuance of supply, and unjustified discrimination. Google’s conduct threatens innovation and investment. It has diminished consumer choice. And it facilitates the continued collection of personal information on the internet. The enumerated abuses are meant to be illustrative and not exhaustive.

8.2. Tying / bundling

356. Tying/upstream products: Google technologically (technically) ties its dominant mobile browser to its dominant mobile operating system, and also technologically (technically) ties its dominant mobile browser to its dominant mobile app store. In addition, Google contractually ties both its mobile browser and its mobile app store to its dominant mobile OS. Moreover, Google uses its dominant mobile application store to provide the enabling access and technology for mobile applications to participate on the dominant Android OS platform. By bundling/tying together these dominant products, Google further enhances its market power. These products together comprise the “tying products.”

357. Google technically ties (technologically incorporates) various aspects of its mobile privacy and security software into its tying products, meaning that consumers get Google’s privacy and security software solutions on their mobile devices whether they want them or not.

---

340 See Case COMP/M.6381 -- Google/Motorola Mobility, 13 February 2012 at paragraph 29 and case COMP/M.7047 Microsoft/Nokia, 4 December 2013.
343 See, e.g., Microsoft/Nokia at paragraph 41 (consumer/communications apps); Case COMP/M.4942 – TomTom/TeleAtlas, 2 October 2008.
344 See, Microsoft (WMP) (Case T-201/04 Microsoft Corp. v. Commission, ECR II – 3620; Article 102 Guidance at paragraph 51. Google, Disconnect, Ghostery and other firms compete in this market.
345 See paragraph 54 of Article 82 Guidance.
346 See generally, Microsoft (WMP) (Case T-201/04, Microsoft Corp. v. Commission, ECR II – 3620).
Consumers cannot get the tying products on their mobile devices without also taking Google’s tied mobile privacy and security software.

358. The effect of ties, particularly in the context of Google’s pattern of conduct and the network effects of the relevant markets, forecloses effective competition from Disconnect in the tied product market. Users tend “to stick to” the installed defaults.  

359. The ties also protects Google’s position in the tying markets in that, as a result of the ties, consumers use Google’s ineffective privacy and security software. This permits Google to exploit its dominant positions by continuing to collect personal data – the “new currency” of the internet. This “new currency” is the method by which Google profits from its tying. The more Google forecloses effective competition from Disconnect, the greater Google’s “profits” in the new currency.

8.3. Refusal to supply

360. Google is dominant in the upstream markets for mobile operating systems and application stores and uses its application store as the only realistic access point to its dominant mobile OS. Google competes against Disconnect in the downstream mobile privacy and security market. Google refuses to supply and/or has unlawfully discontinued supply to Disconnect in at least three ways.

8.3.1. Conduct

361. First, Google has removed Disconnect’s mobile malvertising application from the Play Store and threatened additional punitive actions against Disconnect for further attempts to publish its malvertising technology through the Play Store, after twice accepting and publishing Disconnect’s mobile malvertising application. The termination of an existing supply arrangement increases the likelihood of finding abuse.

362. Second, by removing Disconnect’s application from the Play Store, Google has used its dominance of mobile operating systems and attendant application stores to deny Disconnect the ability to be found (i.e., to be included in the dominant “organic” and “paid” search result mechanisms) by potential customers. This is similar to, if not virtually identical to, charges made by the Commission against Google in the recent Statement of Objections over desktop search results manipulation.

363. Third, by removing Disconnect’s app from the Play Store and threatening further action, Google has denied Disconnect key technology necessary to maintain and improve its products.

---

347 Case COMP/c-3/39530 – Microsoft (Tying) (Commission’s decision accepting revised commitments dated 16.12.2009 at paragraph 63.)
348 See Article 82 Guidance at paragraph 52.
349 See Article 82 Guidance at paragraph 84.
8.3.2. Objectively necessary input

364. As explained throughout this complaint, without participation in the Play Store and receipt of the technology that accompanies participation, Disconnect cannot successfully develop, maintain, sell or distribute mobile privacy and security applications for the Android operating system. Google uses its dominant mobile app store to provide the enabling access and technology for mobile apps to participate on the Android OS platform.

365. Competitors do not provide access to the lion’s share of the mobile OS market. Alternative distribution mechanisms (such as sideloading) do not provide realistic alternatives to participation in the Play Store for access to Android OS users. And Disconnect has been unable to duplicate the features of the denied input, despite the company’s best efforts to do so.\(^{351}\)

8.3.3. Foreclosure

366. Google’s conduct has all but eliminated Disconnect’s ability to provide effective security and privacy protection to Android users. As a result of Google’s conduct: Disconnect has little ability to be found by Android users; Disconnect cannot provide a mechanism by which Android users can easily install Disconnects’ malvertising applications; Disconnect lacks access to technology by which to maintain and improve its products. Indeed, Google’s conduct has produced actual foreclosure, as the financial performance of Disconnect’s malvertising and AiO apps on the Android platform demonstrate. The foreclosure of Disconnect’s products has left Google free to collect user data, a principal method by which internet companies accrue profits.\(^{352}\)

8.3.4. Consumer harm

367. As indicated below, Google’s conduct has impaired the market entry of a new kind of product – effective privacy and security protection on the mobile platform. Google’s conduct has not simply diminished consumer choice and retarded innovation. The conduct has left users vulnerable to exploitation and cybercrime.

8.4. Denigration

368. Google knowingly and repeatedly posts inaccurate and alarming warning messages to users trying to sideload Disconnect’s products. These messages are intended to create unwarranted doubts in the mind of users with regard to the security of Disconnect’s products. The French Competition authority has held that such “publicly discrediting” statements constitute an abuse of dominant position under Article 102.\(^{353}\)

---

\(^{351}\) See Article 82 Guidance paragraph 83.

\(^{352}\) See Article 82 Guidance at paragraph 20.

\(^{353}\) See Decision No. 07-D-33 du 15 Octobre relative a des pratiques mises en oeuvres par France Telecom dans le secteur de l’accès à internet Haut débit at paragraphs 39 –40, 77 – 81.
8.5. Exceptional circumstances

369. To the extent that Google claims that the technology and functionality it has withdrawn from Disconnect are subject to license, the facts herein suffice to demonstrate the “exceptional circumstances” necessary to demonstrate abuse. 354

8.5.1. Neighboring market

370. Google dominates the market for mobile operating systems and mobile app store market that provides the enabling access and technology for apps to participate on the Android OS platform. As demonstrated throughout this Complaint, mobile privacy and security software is a neighboring market dependent upon the technology provided through Play Store participation to compete effectively in the mobile OS market. 355

8.5.2. Refusal Excludes Competition

371. As demonstrated elsewhere in this Complaint, Google’s refusal to provide the contested information precludes effective competition from Disconnect’s malvertising and AiO products. Google’s policy does not preclude all competition in the neighboring market, but it restricts competition to products and solutions that are not effective in protecting user privacy and security. As a consequence of Google’s refusal, Disconnect’s Android malvertising products are relegated to a marginal position and made unprofitable. 356

8.5.3. Refusal prevents new product

372. Google’s refusal to provide the requisite information has literally prevented the appearance of a new product, one that provides effective malvertising protection. 357 Hence, Google’s conduct has limited production, markets or technical developments to the prejudice of consumers. 358

8.6. Unjustified discrimination

373. Unjustified discrimination: Google’s removal of Disconnect’s malvertising app and attendant threats constitute unjustified discrimination against Disconnect, amounting to an abuse of dominant position, in violation of Article 102(c), in that Google has applied dissimilar conditions to “equivalent transactions,” creating a competitive disadvantage for Disconnect. 359

374. As explained in detail in this Complaint, Google’s own technically and contractually tied software, and Ghostery’s mobile browser and mobile application (both available in the Play Store), provide some degree of privacy and security protection to Android users -- albeit less effective and less comprehensive protection than Disconnect does. Yet Google applies neither

354 See Microsoft Judgment.
355 See Microsoft Judgment at paragraphs 207, 369, 229, 381, 387 and 395.
356 See Microsoft Judgment at paragraph 593.
357 See Microsoft Judgment at paragraph 643.
358 See Article 102(b).
its own published rules nor the stated rationale behind those rules to prevent the distribution of either its own privacy and security technology or Ghostery’s through the dominant Google platforms.\(^{360}\)

375. As explained in this Complaint, Google’s discrimination has subjected Disconnect to an enormous competitive disadvantage.\(^{361}\)

### 8.7. No objective justification

376. Google’s pattern of abusive behavior cannot be objectively justified. A dominant company may justify exclusionary conduct by showing that its conduct is “objectively necessary” based on factors external to the company – health and safety reasons related to the nature of the product in question, for example.\(^{362}\) Google tenders no such representations here.

377. Google’s stated reason for removing Disconnect’s app from the Play Store is that the app interferes with the advertising Google sells. Disconnect’s products are intended to improve user security. And interference with the rights of a data subject cannot be justified by a mere economic interest of an operator.\(^{363}\)

378. Moreover, Disconnect’s technology gives European users the ability to avail themselves of the rights to privacy and security that they have under the revised ePrivacy Directive, as applied by the Article 29 Working Party opinions. Google’s interests in making higher profits could not possibly justify undermining those rights.

379. Nor are Google’s actions proportionate or reasonable steps to protect its commercial interests. Disconnect’s products only block unsolicited connections with sites and services that invisibly track users. They do not block sites and services that merely serve ads. So, third party apps can host advertising, and Google can sell that advertising, without getting blocked by Disconnect’s technology, as long as no invisible, nonconsensual tracking is involved.

380. In any case, Google’s stated rationale for removing the malvertising app is inconsistent with its own stated policy, with its continued treatment of Disconnect’s desktop technology, with its treatment of its own privacy and security software, and with the treatment of Disconnect’s competitors – further undermining any defense based on objective necessity.

---


\(^{361}\) See, e.g., Case T-301/04 Clearstream Banking AG v. Commission.

\(^{362}\) See Article 82 Guidance at paragraphs 28–29.

\(^{363}\) See Case C-131/12 Google Spai SL, Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD), Maria Costeja Gonzalez, at paragraphs 80–81.
8.8. No sufficient efficiencies

Google has not claimed that removing Disconnect’s malvertising technology from the Play Store creates any cognizable efficiencies. Google makes no claim that excluding effective privacy and security protection improves the technical quality of its own products, or reduces its costs of production. Google merely claims that Disconnect’s technology reduces Google’s profits—specifically, the ill-gotten gains of violating the privacy rights of Europeans. And given the demonstrable negative effects of Google’s conduct on competition and consumer welfare—basically eliminating effective competition—efficiency claims could not satisfy the Commission’s standards. 364

8.9. Remedies

Google technically ties various aspects of its mobile device privacy and security client software into the Android OS and into the Chrome mobile browser. It also technically ties the Chrome mobile browser into the Play Store and contractually ties the Play Store and the mobile browser (both as part of the Store and as a free-standing app) to the Android OS. And, finally, Google includes Disconnect’s less effective competitors in the Play Store, while denying Disconnect’s malvertising and AiO app participation, technology, etc.

Although Google’s technically tied mobile privacy and security client software lacks effectiveness, as does the software of Disconnect’s competitors that Google continues to include in the Play Store, an unbundling remedy is difficult to administer and may not be necessary.

8.9.1. Equal treatment

Instead, at least at this stage, we ask that the Commission simply enjoin Google from providing to Disconnect’s applications and technology anything less than treatment equal to what Google accords to its own products that include mobile device security and privacy client software, and the products of Disconnect’s mobile device security and privacy client software competitors—with the limited exception of requiring technical tying directly into Google’s mobile OS or mobile browser.

In practical terms, this means restoring Disconnect’s app to the Play Store and accepting the AiO app and similar Disconnect privacy and security apps into the Store—with access to all technology and information provided through the Store, the Android OS or more generally. And, to the extent Google contractually ties the Chrome mobile browser or the Play Store with its Android OS, Google must similarly tie Disconnect’s applications, on the same terms.

The “equal treatment” injunction and obligation should be comprehensive (except as indicated above) and continuing—meaning that as Google changes and “repackages” its technology, whether to evade a Commission order or otherwise, Google must continue to make available to

364 See Article 82 Guidance at paragraph 30.
Disconnect all technology, information, interfaces, etc., that it provides to its own products that contain mobile privacy and security client software, and to Disconnect’s competitors.

8.9.2. Urgency

387. Urgency is required in the imposition of remedial relief, particularly the imposition of injunctive relief of the type described above. Disconnect is a small company with limited resources. Failure to correct Google’s abusive behavior in the near term will cause the company irreparable injury which would likely have the effect of denying Europeans adequate privacy and security protection on the internet.

388. Moreover, unless restrained, Google will continue to discriminate in favor of its own ineffective privacy and security software, as well as the software of Disconnect’s competitors like Ghostery. Google distributes this ineffective software through its products that dominate markets characterized by network effects. So, unless quickly restrained, Google will successfully insinuate ineffective privacy and security software (that will permit the companies to collect personal data) throughout the internet, foreclosing Disconnect’s opportunities with customers.

The information given in this form and in the Annexes thereto is given entirely in good faith.

Date: June 1st, 2015

Casey Oppenheim

Contact information:

Gary L. Reback
Carr & Ferrell LLP
120 Constitution Drive
Menlo Park CA 94025
+650 812-3400
GReback@CarrFerrell.com

Casey Oppenheim
Disconnect Inc.
25 Division Street, 2nd Floor
San Francisco CA 94103
+415 861-9364
Casey@Disconnect.com
Appendix A Correspondence
This is a notification that your application, Disconnect Mobile, with package ID me.disconnect.mobile, has been removed from the Google Play Store.

**REASON FOR REMOVAL:** Violation of section 4.4 of the Developer Distribution Agreement.

After a regular review we have determined that your app interferes with or accesses another service or product in an unauthorized manner. This violates the provision of your agreement with Google referred to above.

This particular app has been disabled as a policy strike. If your developer account is still in good standing, (and the nature of your app allows for it), you may revise and upload a policy compliant version of this application as a new package name.

This notification also serves as notice for remaining, unsuspended violations in your catalog, and you may avoid further app suspensions by immediately unpublishing any apps in violation of (but not limited to) the above policy. Once you have resolved any existing violations, you may republish the app(s) at will. Before publishing applications, please ensure your apps' compliance with the Developer Distribution Agreement and Content Policy.

All violations are tracked. Serious or repeated violations of any nature will result in the termination of your developer account, and investigation and possible termination of related Google accounts. If your account is terminated, payments will cease and Google may recover the proceeds of any past sales and/or the cost of any associated fees (such as chargebacks and transaction fees) from you.

If you feel we have made this determination in error, you can visit this Google Play Help Center article for additional information regarding this removal.

The Google Play Team

On 08/27/14 12:22:48 pat@disconnect.me wrote:

registered_email_address: pat@disconnect.me
abuse_type: other
abuse_type--other: 4.4 of Developer Distribution Agreement
package_name: me.disconnect.mobile
appeal_reason: Our Google Play Developer Console account is still active. We are appealing the removal of one our applications, Disconnect Mobile, which is an essential privacy and security tool. Our technology relies on
the VpnService API made publicly available by Google since API level 14. There are hundreds, if not thousands of other applications that utilize the same API. In addition, we utilize this API to provide a better experience and allow users to enjoy the privacy and security benefits of a VPN without many of the drawbacks associated with VPNs. We are a small startup and spent over a year developing this application, with particular focus on not utilizing any technology that would violate PlayStore guidelines. We believe this removal was erroneous and arbitrary for the reasons stated above and ask that the suspension be lifted. We respectfully request a prompt reply, as I'm sure you can appreciate that being rejected from the PlayStore has been a traumatic experience for our team.

From: <googleplay-developer-support@google.com>
Date: Mon, Sep 8, 2014 at 6:23 PM
Subject: RE: [4-4773000004600] Regarding your Google Play App Suspension Appeal
To: pat@disconnect.me, casey@disconnect.me

Thank you for your note. We apologize for our delayed response. We have reviewed your appeal and are unable to reinstate your app without material revisions to make it compliant with Google Play's policies.

The Disconnect Mobile application interferes with other applications, because it blocks the policy compliant ad serving functionality in third party apps available on the store.

Please note that additional violations in this or additional apps on the store may result in a suspension of your Google Play Developer account. If you have additional apps in violation, you are asked to immediately unpublish them from distribution on Play.

Regards,
The Google Play Team

From: Casey Oppenheim <casey@disconnect.me>
Date: Mon, Sep 8, 2014 at 7:01 PM
Subject: Re: [4-4773000004600] Regarding your Google Play App Suspension Appeal
To: googleplay-developer-support@google.com
Cc: Patrick Jackson <pat@disconnect.me>

Thanks for the additional information.

To make material revisions we need to better understand the meaning of "policy compliant ad serving functionality in third party apps available on the store". Is there documentation or
a specification that defines this? Once we have a better understanding of this term, we will revise the app accordingly and insure compliance if possible.

We look forward to working with you to resolve this quickly.

Casey

From: <googleplay-developer-support@google.com>
Date: Mon, Sep 8, 2014 at 7:32 PM
Subject: RE: [4-4773000004600] Regarding your Google Play App Suspension Appeal
To: Casey Oppenheim <casey@disconnect.me>
Cc: Patrick Jackson <pat@disconnect.me>

Thank you for the reply. The following policy documents may be helpful for your research:

Google Play Content Policy

- System Interference
- Ad Policy

Developer guidance on ads and system interference policies.
Developer guidance on using advertising ID.

It also appears you have published another app, also in identical violation of our terms. In line with the guidance provided in our initial message, please immediately unpublish this app (and any other apps) in violation of Play policies, until you are able to release a policy compliant version.

Regards,
The Google Play Team

From: Casey Oppenheim <casey@disconnect.me>
Date: Mon, Sep 8, 2014 at 8:29 PM
Subject: Re: [4-4773000004600] Regarding your Google Play App Suspension Appeal
To: googleplay-developer-support <googleplay-developer-support@google.com>
Cc: Patrick Jackson <pat@disconnect.me>

Thanks for the prompt reply.
These documents don’t appear to apply to our application, and in fact seem to indicate that our app is compliant. Please specify the exact term that you believe our application violates. We want very much to understand what Google believes needs to be modified.

Clearly, our application’s blocking of known and suspected sources of malware does not violate Play policies.

The removal or temporary suspension of our application at this time will cause significant irreparable damages to our users and Company.

We are a certified public benefit corporation with a mission to protect user privacy and security. We implore you to continue this dialogue and work with us to promptly resolve this matter.

Casey

From: <googleplay-developer-support@google.com>
Date: Mon, Sep 8, 2014 at 10:50 PM
Subject: RE: [4-4773000004600] Regarding your Google Play App Suspension Appeal
To: Casey Oppenheim <casey@disconnect.me>
Cc: Patrick Jackson <pat@disconnect.me>

Hi Casey,

Thank you for your reply. As stated previously, we’ve reviewed both apps and re-affirm both are in violation of Google Play Developer Terms. Apps found in non-compliance will be removed from the store. We’ve provided you an opportunity to voluntarily unpublish me.disconnect.mobile2 while you work through these details, however, failure to remove the app in non-compliance will result in administrative removal, and potential termination of your developer account for repeat violations.

The information we’ve provided in our prior note is in direct response to the specific question in your previous email:
"...we need to better understand the meaning of "policy compliant ad serving functionality in third party apps available on the store". Is there documentation or a specification that defines this? Once we have a better understanding of this term, we will revise the app accordingly and insure compliance if possible."

The policy non-compliance of your application was communicated within the suspension notification of your prior app, me.disconnect.mobile. This violation also applies to the me.disconnect.mobile2 application. After review, they were determined to be in violation of Developer Distribution Agreement 4.4 Prohibited Actions:

"...You agree that you will not engage in any activity with the Market, including the development or distribution of Products, that interferes with, disrupts, damages, or accesses in an unauthorized manner the devices, servers, networks, or other properties or services of any third party including, but not limited to, Android users, Google or any mobile network operator..."

Please note this is a final warning of app removal.

The Google Play Team

From: Google Play Support <googleplay-developer-support@google.com>
Date: Tue, Sep 9, 2014 at 12:03 AM
Subject: Notification from Google Play
To: pat@disconnect.me

This is a notification that your application, Disconnect Mobile, with package ID me.disconnect.mobile2, has been removed from the Google Play Store.

REASON FOR REMOVAL: Violation of section 4.4 of the Developer Distribution Agreement.

After a regular review we have determined that your app interferes with or accesses another service or product in an unauthorized manner. This violates the provision of your agreement with Google referred to above.

Before publishing applications, please ensure your apps’ compliance with the Developer Distribution Agreement and Content Policy.

All violations are tracked. Serious or repeated violations of any nature will result in the termination of your developer account, and investigation and possible termination of related Google accounts. If your account is terminated, payments will cease and Google may
recover the proceeds of any past sales and/or the cost of any associated fees (such as chargebacks and transaction fees) from you.

If you feel we have made this determination in error, you can visit this Google Play Help Center article for additional information regarding this removal.

The Google Play Team

From: Casey Oppenheim <casey@disconnect.me>
Date: Mon, Sep 15, 2014 at 8:32 AM
Subject: Re: [4-4773000004600] Regarding your Google Play App Suspension Appeal
To: googleplay-developer-support <googleplay-developer-support@google.com>
Cc: Patrick Jackson <pat@disconnect.me>

Play team member,

Our app has been removed for a second time and after reading the relevant material we don’t know how to bring it into compliance. We’d like to work with you to avoid any further non-compliant resubmissions.

We understand that we were removed because we block “policy compliant ad serving functionality in third-party apps”. Does this mean to comply we have to unblock all the ad services in our block list, or just some of them?

Also, our block list contains over 2000 known or suspected malware sites, which I assume Google doesn’t have an issue with us blocking, but it would be great to know for sure exactly what the rules are before we resubmit again.

We have received your warning very clearly that removals count as strikes against us and put our developer account in jeopardy. The loss of our Play developer account would cause serious damage to our company.

We have several partnerships that are reliant on our apps being in the Play store in the immediate future. In addition, please take into consideration that our team’s product roadmap relies on knowing whether Disconnect Mobile will be allowed back into Play and under what terms.
Are you or a developer advocate at Play able to speak or engage in a back and forth about how we can modify our app to come into compliance? We look forward to your prompt reply and working with you to resolve this issue.

Thanks,
Casey
(415) 861-9364

On 09/15/14 17:48:50 pat@disconnect.me wrote:

registered_email_address: pat@disconnect.me
abuse_type: dda
package_name: me.disconnect.mobile2
appeal_reason: Our app has been removed for a second time and after reading the relevant material we don't know how to bring it into compliance. We'd like to work with Play to avoid any further non-compliant resubmissions.

We directly emailed the Play team member we were in contact with prior to removal, and hope to hear back soon.

We understand that we were removed because we block "policy compliant ad serving functionality in third-party apps". Does this mean to comply we have to unblock all the ad services in our block list, or just some of them?

Also, our block list contains over 2000 known or suspected malware sites, which I assume Google doesn't have an issue with us blocking, but it would be great to know for sure exactly what the rules are before we resubmit again.

We very much hope to avoid any further strikes against our Play Developer account, and work with you to restore our app to the Play Store. Thanks.
From: <googleplay-developer-support@google.com>  
Date: Thu, Sep 18, 2014 at 12:37 PM  
Subject: RE: [5-1298000004748] Regarding your Google Play app suspension appeal  
To: pat@disconnect.me

Thank you for your note. We apologize for our delayed response. We have reviewed your appeal and will not be reinstating your app. This decision is final and we are unable to respond to any additional emails regarding this removal.

We are unable to comment further on the specific policy basis for this removal or provide guidance on bringing future versions of your app into policy compliance. Instead, please reference the REASON FOR REMOVAL in the initial notification email from Google Play.

Please note that additional violations may result in a suspension of your Google Play Developer account.

The Google Play Team