

Submission to the Australian Competition and Consumer Commission on the proposed acquisition of Fitbit, Inc. by Google LLC

March 2020

privacyinternational.org

24 March 2020

Australian Consumer and Competition Commission (ACCC)
23 Marcus Clarke Street
Canberra ACT 2601
GPO Box 3131
Canberra ACT 2601
By e-mail: mergers@accc.gov.au

Submission re: Google Fitbit-attention Braeden Smith /Nicholas Wellfare:

Privacy International's submission to the Australian Competition and Consumer Commission (ACCC) on the proposed acquisition of Fitbit, Inc. by Google LLC

Introduction

Privacy International (PI) welcomes the ACCC's request for submissions in relation to the proposed acquisition of Fitbit, Inc. (Fitbit) by Google LLC (Google) (the proposed acquisition).

PI is an international charity, based in London, which campaigns against the exploitation of our data and privacy by companies and governments. We expose harm and abuses, mobilise allies globally, campaign with the public for solutions to end the exploitation of data, and pressure companies and governments to change behaviour.

PI employs technologists, investigators, policy experts, and lawyers, who work together to understand emerging technology and to consider how existing legal definitions and frameworks map onto such technology. We are frequently called upon to give expert evidence to parliamentary and governmental committees around the world and have advised, and reported to, among others, the Parliament of the United Kingdom, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

In recent years, PI has conducted extensive research into online platforms and the AdTech industry, as part of its Corporate Exploitation Programme, exposing[1] and complaining[2] about several companies' exploitation of personal data and the lack of transparency of their activities. We have also submitted evidence to the UK Competition and Markets Authority,[3] the European Commission[4] and the U.S. Federal Trade Commission[5] regarding data and competition issues.

Based on our research and analysis of the current trends, this submission provides PI's views on the impact of the proposed acquisition on competition in the relevant markets. The submission covers a number of the issues on which views are sought by the ACCC, including: the impact of the proposed acquisition on prices and features of wearables including the wearable operating system; the ability to foreclose or otherwise frustrate the ability of other businesses to compete; the impact that Google's increased access to data will have on markets which rely on the collection of data, e.g. advertising markets; and the impact of Google extending its "ecosystem" of products.

This submission is structured in three parts. First, we briefly underline the way personal data contributes to the corporate concentration of digital platforms, including Google. We also discuss Google's, and other tech companies', past and on-going projects, acquisitions and general efforts to enter the insurance/health data sector. This could potentially indicate Google's desire to expand their reach into these markets by acquiring vast amounts of sensitive personal data, which at the same time are afforded enhanced protections under data protection laws.[6]

[1] See PI, How Apps on Android Share Data with Facebook – Report, 29 December 2018, https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report.
[2] See PI, Challenge to Hidden Data Ecosystem, https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem.
[3] PI, Submission to the Competition and Markets Authority's call for information on digital mergers, 23 July 2019, https://privacyinternational.org/node/3097; Response to the CMA's online platforms and digital advertising market study, 29 July 2019, https://privacyinternational.org/advocacy/3101/response-cmas-online-platforms-and-digital-advertising-market-study.
[4] PI, Privacy International's submission to the European Commission consultation on 'shaping competition policy in the era of digitisation', 2 October 2018, https://privacyinternational.org/advocacy/2312/privacy-internationals-submission-european-commission-consultation-shaping.
[5] PI, Submission to the US Federal Trade Commission on the intersection between privacy, big data, and competition, 1 August 2018, https://privacyinternational.org/report/2262/submission-us-federal-trade-commission-intersection-between-privacy-big-data-and.
[6] Sensitive data, such as health data is afforded heightened protections in data protection regimes around the world, meaning that without the proposed acquisition it could only be shared with Google in very limited and unlikely scenarios. See, for example, article 9 EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), which prohibits the processing of, among others, special-category data such biometric data as well as "*data concerning health or data concerning a natural person's sex life or sexual orientation*", unless strict and limited exceptions apply. The Australian Privacy Act also includes health or genetic information as sensitive information.

Second, we focus on the detrimental effects that the proposed acquisition is likely to have on consumers whose rights might be infringed by data exploitative and/or abusive practices, as well as competitors and other businesses which may face major restrictions to enter or be excluded from entry into the general search, the mobile device operating system and the online advertising markets.

Finally, taking into account Google's history in relation to compliance with data protection and competition laws, as well as its failure to live up to its promises before regulators,[7] it is our view that the proposed acquisition will grant Google unprecedented access to sensitive personal data and is likely to have the effect of substantially lessening competition in markets such as the general search market, digital advertising market, as well as health/insurance markets. We therefore ask the ACCC to prohibit the proposed acquisition in accordance with its powers under section 50 of the Competition and Consumer Act 2010.

The value of data in the digital economy and Google's market power

In the digital economy there is a trend towards corporate concentration. This is particularly true for digital platforms, such as social media platforms, search engines, digital entertainment, or online retailers. Traditionally, the way in which market dominance is measured does not always capture the extent of these companies' market power, as their products and services are often 'free' to consumers.

This trend is fuelled by the increasing reliance of many sectors of the economy on data, particularly personal data. Personal data is increasingly valuable in the digital economy. It is widely acknowledged that individuals' data is the most important asset in the digital economy and the acquisition of vast quantities of data is what allows companies like Google to make billions of dollars each year via targeted advertising. In 2018, for example, Google's parent company, Alphabet, generated 85% of its $136.22 billion in revenue from delivering targeted advertisements to the users of their many user-facing services, which include the Android operating system, Google Search, YouTube, Gmail, and many others.[8]

The value of personal data increases as more and more data is combined, and this incentivises companies to pursue business strategies aimed at collecting as much data as possible.[9] With the development and integration of artificial intelligence technologies, it is

[7] PI, Google merges privacy policies and data across services, 25 January 2012, https://privacyinternational.org/examples/2178/google-merges-privacy-policies-and-data-across-services.
[8] United States Securities and Exchange Commission, Alphabet Inc. Annual Report pursuant to section 13 or 15(d) of the Securities Exchange Act of 1934 (For the fiscal year ended December 31, 2018), https://abc.xyz/investor/static/pdf/20180204_alphabet_10K.pdf?cache=11336e3.
[9] Maurice Stucke and Allen Grunes, *Big Data and Competition Policy*, 2016 Oxford University Press.

likely that users' data will become even more important for these companies, since their data is an essential input to train AI models. And given the growing importance of data across all sectors of the economy, the concentration is likely to continue and expand to other markets.

The effects of this concentration of power are significant, and they are not limited to online and offline privacy. Companies like Google act as gatekeepers, for example by regulating how we access information on the web as well as which applications can we install on our devices. They can track and profile us across devices to predict and influence our behaviour. This is no longer 'just' affecting the realm of digital advertising. Increasingly corporate powers encroach on the functioning of democracy and have profound societal impacts.

At the same time, companies exploiting personal data often view privacy and data protection legislation as a threat to their business models. For instance, Alphabet Inc.'s 2017 Annual Report to the US Securities and Exchange Commission notes similar concerns and specifically states in relation to data protection regulation that "*these legislative and regulatory proposals, if adopted […] could, in addition to the possibility of fines, result in an order requiring that we change our data practices, which could have an adverse effect on our business and results of operations. Complying with these various laws could cause us to incur substantial costs or require us to change our business practices in a manner adverse to our business.*"[10]

Given the value of data in the digital economy and indeed the concentrations of power which already exist, it is of utmost importance that an undertaking's data holding is taken into account for the purposes of competitive assessments of market power. Indeed, the importance of data holding is very well-recognised by the tech giants, like Google, who consistently seem to regard consumers' data as a business asset[11]. It is also absolutely integral to these companies' market value. We note that it is also an asset which is all the more valuable when a digital service provider is able to combine data from multiple sources, including across multiple services or platforms.

Therefore, the ability to deal appropriately with concentrations of data is key to the evolution of competition rules to deal with the challenges of the digital economy: it ought, in our view, to be a default starting point from which any departures would need to be fully justified (if indeed any could be). As the German competition authority (Bundeskartellamt) noted in its February 2019 decision against Facebook:

[10] United States Securities and Exchange Commission, Alphabet Inc. Annual Report pursuant to section 13 or 15(d) of the Securities Exchange Act of 1934 (For the fiscal year ended December 31, 2017), https://abc.xyz/investor/pdf/20171231_alphabet_10K.pdf.
[11] European Data Protection Supervisor (EDPS), Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 September 2016, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.

"*Monitoring the data processing activities of dominant companies is therefore an essential task of a competition authority, which cannot be fulfilled by data protection officers. In cases of market dominance a competition authority must take into account data protection principles, in particular in the assessment of whether terms and conditions for the processing of data are appropriate*."[12]

Our investigations reveal that data exploitation tends to be perpetrated by companies which occupy dominant positions in the various online markets, and we believe that competition rules have a vital role to play in holding the digital giants to account. We particularly welcome the ACCC's decision to investigate Google's proposed acquisition of vast quantities of sensitive, health-related data – indeed we hope that this scrutiny presents an opportunity to prevent further and greater economic harms, to consumers and to society as a whole.

In the 2019 Final Report of its Digital Platforms Inquiry, the ACCC found that Google enjoyed substantial market power in the supply of general search services, the supply of search advertising services as well as substantial bargaining power in its dealings with news media businesses in Australia.[13] The report further noted:

"There are high barriers to entry and expansion in the markets for the supply of general search and search advertising services and data plays a key role in these barriers. For example, there are network effects from Google's ability to accumulate large quantities of user data that it can then use to improve its online search and search advertising services.

Google also enjoys advantages of scope in accumulating data from consumers using its wide range of services, including Google Search, Google Maps, YouTube and Gmail; and most mobile phones that use the Android operating system. The advantages are compounded by Google's ability to track consumers on the more than two million websites that use Google advertising services or offer sign-in options through Google.

Google's position across a range of markets, such as mobile operating systems (Android), and web browsers (Chrome), enables Google to set Google Search as a default option. As consumers infrequently change defaults, this has the effect of further

[12] Bundeskartellamt, Bundeskartellamt prohibits Facebook from combining user data from different sources, Background information on the Bundeskartellamt's Facebook proceeding, 7 February 2019, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf.

[13] Australian Competition and Consumer Commission (ACCC), Digital Platforms Inquiry, Final Report, June 2019.

entrenching its market power. As set out above, while the data collected by Google increases its market power, the market power held by Google and its presence across related markets can also enable it to collect greater quantities and qualities of data.

Strategic acquisitions also appear to have performed an important role in entrenching Google's position in search and search advertising. Through a series of acquisitions, Google has obtained further advantages of scope and reduced potential competition. By expanding into related markets, Google has been able to remove possible rivals to its core products which, in the medium term, weakens the constraints from dynamic competition.

The ACCC has also identified that substantial economies of scale and sunk costs and the strength of Google's brand are barriers to entry and expansion.

These high barriers to entry and expansion underpin Google's substantial market power and its significant share of relevant markets. At the time of writing, approximately 95 per cent of general searches in Australia are performed through Google and Google earns almost 96 per cent of all search advertising revenue in Australia."[14]

Similar conclusions about Google's market power and the role that the vast quantities of user data the company processes are drawn in the UK Competition and Markets Authority's (CMA) interim report into its online platforms and digital advertising market study. While acknowledging that "*Google enjoys a more than 90 % share of the £6 billion search advertising market in UK*", the interim report found that *Google has significant market power both "in the general search sector, having had a share of supply of around 90% or higher in the UK for more than a decade*"[15] as well as "*in search adverting*".[16] The interim report underlined:

"Google's strong position is primarily maintained by three key barriers to entry and expansion: economies of scale in developing a web index, access to click -and- query data at scale, and Google's extensive default positions across desktop and mobile devices.[17]

[14] Ibid.
[15] Competition and Markets Authority (CMA), Online platforms and digital advertising, Market study interim report, December 2019.
[16] Ibid.
[17] Ibid.

Google is also able to use its access to data across a large proportion of the internet to provide higher-quality analytics and attribution services which increases the value of the advertising in a way that is very hard for other smaller search providers to compete with. These factors are reflected in the higher revenues per user that Google is able to earn relative to its competitors.[18]

The value of Fitbit's personal data improving Google's data driven services and power in various markets

PI strongly believes that the proposed acquisition will further strengthen Google's dominance in the general search and digital advertising markets, and will also allow Google to expand and gain significant power potentially in health and/or insurance markets.

Fitbit is a company that produces and sells health tracking technologies and wearables including smartwatches, health trackers, smart scales and other health tracking services including via mobile.[19] In 2019 Fitbit reported a revenue of $ 1,435 billion.[20]

A big part of Fitbit's value is said to lie in the quality of the health data it possesses.[21] The company's technologies can track individuals' daily steps, distance walked or travelled, calories burned, sleep patterns and heart rate.[22] In 2018, Fitbit also introduced 'female health tracking' to track menstruation cycles and likely fertility windows.[23] In the recent past, Fitbit has further increased its health-related database and health tracking capabilities by acquiring a number of other actors on the health tracking and wearables market, including FitStar, Pebble, Vector and Twine Health. Some of these acquisitions include partnerships with health insurers,[24] as part of efforts to diversify its revenue stream.[25]

Based on Fitbit's privacy policy, the table below illustrates some data categories collected by Fitbit, the personal data involved, and potential ways these data could further strengthen

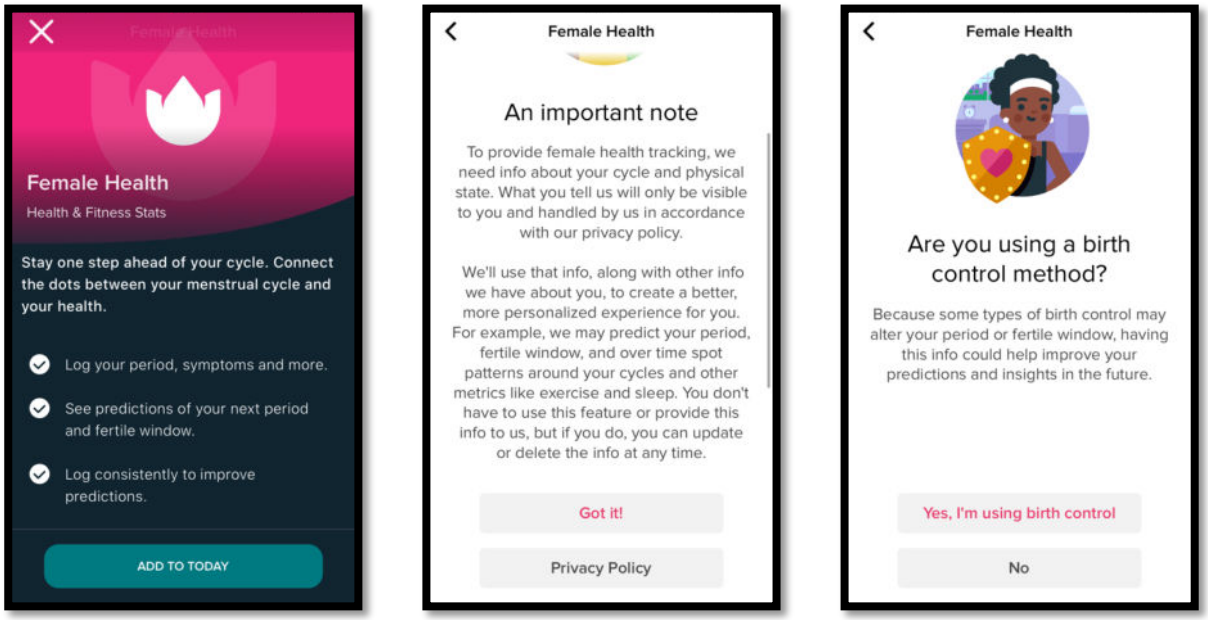
[18] Ibid.
[19] https://www.fitbit.com.
[20] United States Securities and Exchange Commission, Fitbit Inc. Annual Report pursuant to section 13 or 15(d) of the Securities Exchange Act of 1934 (For the fiscal year ended December 31, 2019), http://d18rn0p25nwr6d.cloudfront.net/CIK-0001447599/a8b5d236-bb56-4a1e-9b04-04ffd5e5ee83.pdf.
[21] Michael Sawh, 5 reasons why Google just bought Fitbit, TechRadar, 4 November 2019, https://www.techradar.com/uk/news/5-likely-reasons-why-google-just-bought-fitbit.
[22] Fitbit, Fitbit Privacy Policy, Effective 18 December 2019, https://www.fitbit.com/au/legal/privacy-policy#info-we-collect.
[23] Danielle Kosecki, One of Your Most Requested Features is Here! Introducing Female Health Tracking, Fitbit News, 20 May 2018, https://blog.fitbit.com/female-health-tracking.
[24] Andrew Boyd, Could Your Fitbit Data be used to Deny You Health Insurance?, The Conversation, 17 February 17 2017, https://theconversation.com/could-your-fitbit-data-be-used-to-deny-you-health-insurance-72565.
[25] Mark Sullivan, How Fitbit is trying to transform healthcare, and itself, Fast Company, https://www.fastcompany.com/40578138/how-fitbit-is-trying-to-transform-healthcare-and-itself.

Google's dominance in the general search and digital advertising sector as well as establish significant market power in the health related or insurance markets.

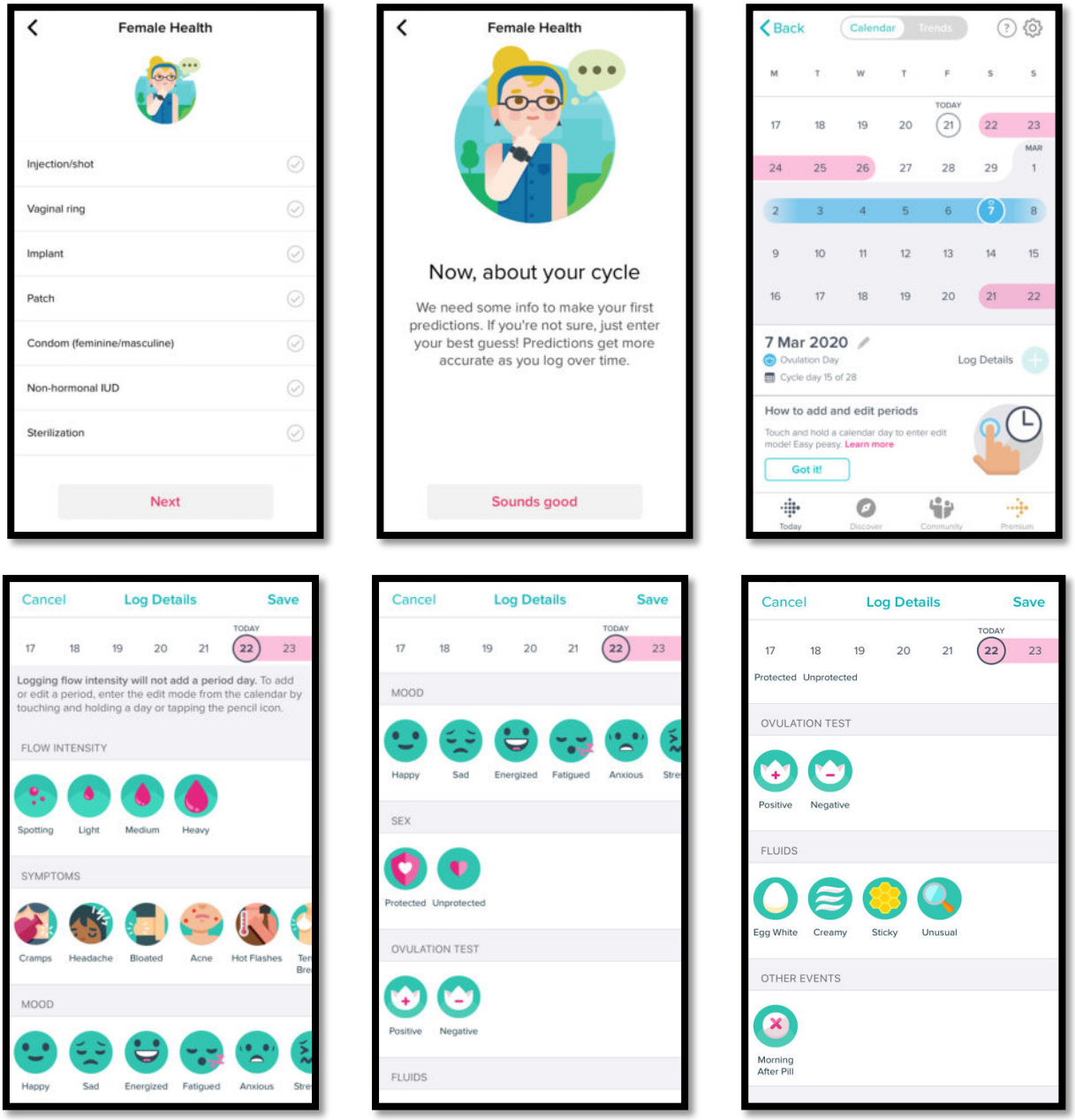
Categories of personal data collected by Fitbit (including sensitive personal data)	**Examples of personal data collected based on Fitbit's privacy policy**	**Market/Sector where Google might enjoy significant dominance**
Geolocation information	"*precise geolocation data, including GPS signals, device sensors, Wi-Fi access points, and mobile mast IDs*"	General search market Search advertising Health products/services sector Insurance sector
Live coaching services	"*goals and actions you record with your coach, your calendar events, communications with your coach, notes your coach records about you, and other information submitted by you or your coach*"	
Device information	"*Your device collects data to estimate a variety of metrics like the number of steps you take, your distance travelled, calories burned, weight, heart rate, sleep stages, active minutes and location*"	
Usage information	"*information about your interaction with the Services, for example, when you view or search content, install applications or software, create or log into your account, pair your device to your account, or open or interact with an application on your Fitbit device.* *We also collect data about the devices and computers you use to access the Services, including IP addresses, browser type, language, operating system, Fitbit or mobile device information (including device and application identifiers), the referring web page, pages visited, location."*	

The wealth of information is vast considering the nature and extent of personal data as well as the fact that in 2019 Fitbit sold a total of about 15.99 million devices and had a total of about 29.57 million active users.[26] Taking into consideration both the amount and sensitivity of the data, we believe that the proposed acquisition would further entrench Google's existing significant market power in the aforementioned markets and also effectively allow Google to establish itself as an even stronger player in the markets for health data-related services including health tracking devices. In short, this could be achieved by potentially merging Fitbit's customer data and/or datasets with the ones held by Google, allowing the latter to enrich the extensive datasets and detailed consumer profiles it holds with sophisticated real time data about individuals' health conditions and needs, as well as general information about their daily behaviour and bodily rhythms.

In other words, the Fitbit data will provide Google with an opportunity to better train its algorithmic models, which among other things, could use these data to better map general search queries originating, for instance, from an extremely specific geographic area/location, or be able to offer advertisers ever more valuable insights into specific audiences by allowing the targeting of the latter based on health conditions, activity level as well as emotional attributes. For example, as noted above, Fitbit also provides users with menstruation tracking features which ask users to provide information about their menstruation cycles, symptoms, whether they are having protected or unprotected sex, what kind of birth control they are using/ if any, their mood etc.



[26] United States Securities and Exchange Commission, Fitbit Inc. Annual Report pursuant to section 13 or 15(d) of the Securities Exchange Act of 1934 (For the fiscal year ended December 31, 2019), http://d18rn0p25nwr6d.cloudfront.net/CIK-0001447599/a8b5d236-bb56-4a1e-9b04-04ffd5e5ee83.pdf.



Screenshots of various notices a user receives as well as examples of personal data a user could provide regarding their menstruation cycle

At this point, we refer to two recent PI investigations.

The first one relates to a PI study that reveals how popular mental health websites in France, Germany and the UK share user data with advertisers, data brokers and large tech companies, including Google, while some 'depression tests' on these websites leak answers and test results to third parties.[27] As the report sets out, the findings raise serious concerns about compliance with European data protection and privacy laws. Although not the focus of the study, such practices may also raise concerns from an Australian legal perspective.

[27] PI, REPORT: Your mental health for sale, 3 September 2019, https://privacyinternational.org/campaigns/your-mental-health-sale.

This research also shows the dominance of Google in this tracking ecosystem. On the webpages we analysed Google is the most prevalent third-party tracker and Google's advertising services DoubleClick and AdSense are used by the vast majority of these webpages. 70.39% of the webpages used DoubleClick. Other Google products such as Google Analytics, Google Tag Manager and Google Fonts are also widely used. 87.8% of webpages in France had a Google tracker, 84.09% in Germany and 92.16% in the UK. Some of the 'depression tests' use programmatic advertising with Real-Time Bidding, which illustrates that Google can also play a role in the processing of highly sensitive data. For example, as part of an RTB prebid request, the French website Doctissimo.fr sends content keywords (such as 'dépression', 'déprimé' (depressed), or 'quizz'), the page URL (psychologie/tests-psycho/tests- psychologiques/coup-de-blues-ou-depression), as well as information about the page content ('psychologie', 'test psychologiques', 'coup de blues ou dépression ?') to the page https://europe- west1-realtime-logging-228816.cloudfunctions.net/realtime-logs (a cloud function hosted by Google that will process the request).

The second report focuses on menstruation apps, which are not just concerned with menstruation cycles but may also collect information about users' health, sexual life, mood etc. Due to the sensitivity of this information, PI looked into whether any of these special-category data were shared with third parties without users' consent or even knowledge. As the report exposes, several apps conducted – at the time of the research – extensive sharing of sensitive personal data with third parties, including Facebook.[28] This indicates the importance of this data for advertisers (and thus for Google) in order to provide better audience insights.

These examples demonstrate that it is vital to consider the proposed acquisition in the context of all consumers' wellbeing in the digital era, by assessing their needs, as well as respecting dignity and preventing the risk of social exclusion and stigmatization of certain groups and minorities.

Additionally, the proposed acquisition does not only signal an effort by Google to increase the profitability of its business model by collecting ever more personal data but also adds to the company's efforts to enter health and/or insurance markets, as illustrated by the following examples.

[28] PI, No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data, 9 September 2019, https://www.privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data.

In January 2016, the European Commission was notified of a proposed concentration by which Sanofi SA ('Sanofi', France) and Google, the latter through its wholly-owned subsidiary Verily Life Sciences LLC, planned to acquire joint control of a newly created company constituting a joint venture, by way of purchase of shares. Sanofi is a global pharmaceutical group engaged in the research, development, manufacture and marketing of healthcare products. In particular, Sanofi offers a range of solutions for the treatment of diabetes. Verily was established in order to group together Google's life sciences related projects. The joint venture would offer services for the management and treatment of diabetes. In addition, the joint venture may commercialise certain products (such as specialised continuous glucose monitoring devices, insulin pumps and insulin) which can be used alongside the services.[29]

In 2015, Royal Free Hospital (RFH) in the UK shared 1.6 million records with DeepMind AI, which had been acquired by Google's parent company, Alphabet, in 2012.[30] The UK's data protection regulator, the Information Commissioner's Office (ICO), ruled that the Royal Free NHS Foundation Trust broke data protection laws when it participated in a trial of Streams, a healthcare application, that used the data of 1.6 million patients without informing them.[31]

In June 2018, a panel set up to examine the partnerships between Alphabet's DeepMind and the UK's National Health Service expressed concern that the revenue-less AI subsidiary would eventually have to prove its value to its parent. As reported by the Financial Times, panel chair Julian Huppert said DeepMind should commit to a business model, either non-profit or reasonable profit, and noted the risk that otherwise Alphabet would push the company to use its access to data to drive monopolistic profits. In that case, DeepMind would either have to produce substantial revenues or share its data and algorithms.[32]

Google also has a research agreement with Mayo Clinic in the US for use of their Cloud; and Google can access anonymised patient information to train algorithms.[33] Finally, in November 2019, a few days after the announcement of the proposed acquisition, it was reported that Google was collecting health data records as part of a project it has

[29] Official Journal of the European Union, Prior notification of a concentration (Case M.7813 — Sanofi/Google/DMI JV) (Text with EEA relevance) (2016/C 28/06), 26 January 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.028.01.0005.01.ENG&toc=OJ:C:2016:028:FULL.
[30] Hal Hodson, Revealed: Google AI has access to huge haul of NHS patient data, New Scientist, 29 April 2016, https://www.newscientist.com/article/2086454-revealed-google-ai-has-access-to-huge-haul-of-nhs-patient-data/#ixzz6HdnLPQQp.
[31] Information Commissioner's Office (ICO), Royal Free - Google DeepMind trial failed to comply with data protection law, 3 July 2017, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law.
[32] Financial Times, Alphabet AI unit urged to clarify its business model, https://www.ft.com/content/215062da-6fe3-11e8-852d-d8b934ff5ffa.
[33] Thomas Kurian, How Google and Mayo Clinic will transform the future of healthcare, Google Cloud, 10 September 2019, https://cloud.google.com/blog/topics/customers/how-google-and-mayo-clinic-will-transform-the-future-of-healthcare.

named "Project Nightingale".[34] This was part of an agreement Google had with Ascension, a Catholic chain of 2,600 hospitals, doctors' offices and other facilities and one of the US's largest health-care systems,[35] whose immense scope purportedly allowed Google to amass data for about a year on patients in 21 US states in the form of lab results, doctor diagnoses and hospitalization records, among other categories, which amount to a complete health history, including patient names and dates of birth.[36]

Google is not the only big tech company wishing to enter health related markets. Sensitive health data are also collected by Apple via its "Health app", which can consolidate data from users iPhones, Apple Watches and third-party apps they already use.[37]

In July 2019, the UK NHS announced that it was teaming up with Amazon "to allow elderly people, blind people and other patients who cannot easily search for health advice on the internet to access the information through the AI-powered voice assistant Alexa".[38] After submitting a series of Freedom of Information Requests, PI was able to obtain a copy of the contract between Amazon and the UK Department of Health. While the largely redacted contract underlined that no patient records are shared with Amazon, we believe that Amazon is still able to amass large quantities of health related data due to the user generated queries around symptoms and health conditions.[39] This could accordingly provide Amazon with opportunities to train algorithmic models in an effort to strengthen its existing dominance in certain markets or even enter health markets. In January 2020, CNBC reported that Amazon bought an Internet pharmacy business called PillPack in 2018 and that it "has filed to trademark "Amazon Pharmacy" in Canada, the U.K. and Australia, signalling a potential move into selling prescription drugs outside of the U.S".[40]

PI underlines the sensitive nature of health-related data including data that can be inferred regarding individuals' conditions, illnesses, health status, mental health, disabilities etc and the consequences of this data gathering, sharing, retention and further use can have on

[34] Rob Copeland, Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans, The Wall Street Journal, 11 November 2019, https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790.
[35] Tariq Shaukat, Our partnership with Ascension, Google Cloud, 11 November 2019, https://cloud.google.com/blog/topics/inside-google-cloud/our-partnership-with-ascension.
[36] PI, Give Google an inch and they'll take a mile!, 13 November 2019, https://privacyinternational.org/node/3280.
[37] See Apple, Health app, https://www.apple.com/uk/ios/health.
[38] Haroon Siddique, NHS teams up with Amazon to bring Alexa to patients, The Guardian, 10 July 2019, https://www.theguardian.com/society/2019/jul/10/nhs-teams-up-with-amazon-to-bring-alexa-to-patients.
[39] PI, Alexa, what is hidden behind your contract with the NHS?, 6 December 2019, https://privacyinternational.org/node/3298.
[40] Christina Farr, Amazon just filed a bunch of international trademarks for 'Amazon Pharmacy', CNBC, 21 January 2020, https://www.cnbc.com/2020/01/21/amazon-files-trademarks-for-amazon-pharmacy-in-uk-australia-canada.html.

people's lives both today and in the future. Any acquisition of such data, not least in the name of profit, must be scrutinised in depth.

The proposed acquisition will likely have the effect of substantially lessening competition in at least the general search market and digital advertising market

In a competitive market, it should be expected that the level of data protection offered to individuals would be subject to genuine competition, i.e. companies would compete to offer privacy friendly services.[41] However, in a data-intensive digital market characterised by increased corporate concentration, companies in a dominant position have no incentive to adopt business models and practices that enhance individuals' privacy, and they may seek to exclude privacy enhancing players from any of the markets where they can exert market power. We believe that such will likely be the case if the proposed acquisition is approved.

Effect on consumers

PI would like to draw the attention of the ACCC to the recent statements made by the European Data Protection Board (EDPB), the EU body comprising EU Member State data protection authorities, in reaction to the proposed acquisition. Specifically, the EDPB highlighted that "the possible further combination and accumulation of sensitive personal data regarding people in Europe by a major tech company could entail a high level of risk to privacy and data protection".[42]

Competition in digital markets can take place along various price and non-price parameters, with examples of the latter being quality, innovation and privacy. The importance of non-price parameters to be expected as the 'price' for service usage which consumers must pay is more often than not that of their data.

As Professor Tommaso Valletti noted before the US House of Representatives Judiciary Committee Subcommittee on Antitrust, Commercial, and Administrative Law in October 2019[43], privacy is at the heart of the economics of the digital platforms and competition is

[41] In its 2014 assessment of the proposed merger of Facebook and WhatsApp (Case No. COMP/M.7217), the European Commission acknowledged that "*competition on privacy*" exists. It stated that "*apps compete for customers by attempting to offer the best communication experience*," including with respect to "*privacy and security, the importance of which varies from user to user but which are becoming increasingly valued, as shown by the introduction of consumer communications apps specifically addressing privacy and security issues*," http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.
[42] European data Protection Board (EDPB), Eighteenth EDPB Plenary Session, https://edpb.europa.eu/news/news/2020/eighteenth-edpb-plenary-session_en.
[43] Testimony of Tommaso Valletti, Before the House Judiciary Committee, Subcommittee on Antitrust, Commercial, and Administrative Law, On "Online Platforms and Market Power Part 3: The Role of Data and Privacy in Competition", 18 October 2019, https://docs.house.gov/meetings/JU/JU05/20191018/110098/HHRG-116-JU05-Wstate-VallettiT-20191018.pdf.

shaped around it. It follows that where there is little competition, quality is degraded, particularly through reductions in users' privacy. The entrenched dominance of the tech giants leaves them with no incentive to adopt practices that enhance individuals' privacy in any meaningful way - rather the opposite; and there is no competitive constraint on their behaviour.

Service quality reductions in the form of lower standards of privacy protection can cause objective detriment to consumers in the form of discriminatory behaviour, profiling, targeting and attempts at manipulating behaviour. For instance, consumers may be served targeted advertising based on their income or vulnerability. Any perceived advantages of targeted advertising should be weighed against these undesirable aspects, we would say as part of the competition analysis.

While such concepts and theories of harm may be described by some as 'novel', we believe that both competition law and the goals of competition policy are sufficiently broad and flexible to encompass a consumer welfare standard which incorporates the metric of privacy. Indeed, it is vital that regulators' and policymakers' interpretation of the consumer welfare standard adapts sufficiently to this reality of the digital economy – specifically, the consumer welfare standard must by default take into account an assessment of privacy rights and data security.[44]

With their business model relying increasingly on the availability of consumers' data, dominant online platforms can engage in various forms of data exploitation or even impose unfair terms for consumers.[45] In its statement on the data protection impacts of economic concentration, the European Data Protection Board (EDPB) has noted that the increase in the digital markets' concentration "*has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services*".[46]

[44] The 'rights' aspect of any such analysis is vital because, as we have consistently highlighted, privacy and data protection are fundamental rights, recognised in various international, regional and domestic instruments. See, for example, Article 12, United Nations Declaration of Human Rights (UDHR) 1948; Article 17, International Covenant on Civil and Political Rights (ICCPR) 1966; Article 11 of the American Convention on Human Rights; Article 8 of the European Convention on Human Rights; Council of Europe Convention 108 for the Protection of Individuals with Regard to the Automatic Processing of Personal Data; Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2004.

[45] See, for example, the class action lawsuit launched by the French consumer rights group UFC-Que Choisir against Google, https://www.quechoisir.org/action-ufc-que-choisir-vie-privee-donnees-personnelles-action-de-groupe-contre-google-n68403/.

[46] European Data Protection Board (EDPB), Statement of the EDPB on the data protection impacts of economic concentration, August 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf.

At the users' level, consumers do not know how their personal data is collected, used and shared with other parties; nor do they know when they have been tracked and profiled.[47] Because users' data is a valuable commodity (a "*proxy for price*", as noted by the European Data Protection Supervisor),[48] dominant online platforms increasingly continue to find ways to obtain yet more data in order to maintain and expand their control on the general search market and the digital advertising market with the likely effect of substantially lessening competition in these markets.[49]

When faced with a demand to consent to the terms of service and privacy policy by a company in a dominant position, users often have no genuine choice but to accept. This lack of choice is caused by a combination of factors: the significant relevance of network effects in these markets -where the utility of a service increases the more people use it, meaning that entrants require a 'critical mass' of users in order to compete, while users may only use the competing service when it has been generally adopted - which consequently erects huge barriers to entry; lock-in of users; lack of alternatives; imposition of terms and conditions with poor privacy safeguards. [50] Companies such as Google continue to impose terms and conditions on users which allow them to collect, analyse and share personal data in ways that people do not understand (or cannot genuinely consent to).[51]

Privacy intrusive default settings, deceptive designs, vague or misleading language and threats of downgrading the service are just some examples of abuses and signal how

[47] Dotveryone, People, Power and Technology, The 2018 Digital Understanding Report, https://doteveryone.org.uk/report/digital-understanding/.
[48] European Data Protection Supervisor (EDPS), Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 September 2016, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.
[49] For instance, in 2015 Facebook was fined by the Belgian Data Protection Authority ("DPA") for tracking the online activities of Belgian non-Facebook users through social plug ins (such as the like-button), cookies and invisible pixels on third-party web sites, https://www.dataprotectionauthority.be/news/judgment-facebook-case. The Belgian DPA's action was based on KU Leuven University's research revealing that Facebook's privacy policies breach European law. This comprehensive study, drafted at the request of the Belgian Privacy Commission, outlines the different data collection techniques, such as cookies, pixels, social plug-ins and other similar technologies used by Facebook to build up user and non-user profiles, see https://www.law.kuleuven.be/citip/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation. The Belgian DPA's decision was challenged by Facebook on grounds of jurisdiction, however in February 2018 the Belgian Court of First Instance once again ruled that Facebook violated privacy laws, by deploying technology such as cookies and social plug-ins to track internet users across the web. The court ordered Facebook to stop tracking Belgians' web browsing habits and destroy any illegally obtained data, https://www.dataprotectionauthority.be/news/victory-privacy-commission-facebook-proceeding. In 2017, Facebook was also fined by the French Data Protection Authority (CNIL) for different privacy violations, among them "unfair" tracking of users and non-users as they browse the internet, without offering users sufficient warning, https://www.ft.com/content/10f558c6-3a26-11e7-821a-6027b8a20f23.
[50] See, for example, WhatsApp forcing its users to accept new terms and conditions that led to the sharing of personal data with Facebook, https://www.theverge.com/2017/5/18/15657158/facebook-whatsapp-european-commission-fine-data-sharing.
[51] See, for example, the complaints filed by noyb – the European Center for Digital Rights against Facebook, Google, WhatsApp and Instagram. The complaints, which were filed on behalf of consumers across the EU, allege that these four companies were violating users' data protection rights by "forcing" them to agree to abusive and bundled data exploitation practices, https://noyb.eu/4complaints.

consumers' privacy can be undermined in the online market.[52] Accordingly, they raise serious transparency concerns, as consumers will very often be unaware of the extent of the collection and use of their personal data, allowing platforms to extract data from them.

In a report dated December 2018, PI revealed how Facebook routinely tracks users, non-users and logged-out users outside its platform through Facebook Business Tools.[53] Facebook is not the only or greatest offender in this respect and Google's role in tracking on apps is even greater. Indeed, PI's study followed a paper by academics at the University of Oxford that outlined the prevalence of third-party trackers on almost 1 million apps from the US and UK Google Play stores. They found that most apps contain third party tracking and the distribution of trackers is long tailed with several highly dominant trackers accounting for a large portion of coverage, with the most prevalent being Alphabet and subsidiaries, with Google present on 87.57% of Apps tested.[54]

A report by Digital Content Next found that "*a major part of Google's data collection occurs while a user is not directly engaged with any of its products*."[55] The report also showed that anonymised data collected by Google through passive methods, could still be associated with personal data of users through advertising.[56]

Considering that the Android operating system is the most widely used worldwide with more than 2 billion users, this raises significant concerns around the magnitude of the personal data collected, as well as the potential implications the proposed acquisition will have in relation to wearables' operating system. The CMA interim report noted that "*Google is able to gain data from mobile devices running the Android operating system, which gives Google a significant advantage in relation to specific types of consumer data such as location data*."[57]

[52] See, for example, Forbukerradet, Deceived by Design, How tech companies use dark patterns to discourage us from exercising our rights to privacy, 27 June 2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.
[53] PI, How Apps on Android Share Data with Facebook (even if you don't have a Facebook account), December 2018, https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf.
[54] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N., Third Party Tracking in the Mobile Ecosystem, arXiv, 2018, https://arxiv.org/pdf/1804.03603.pdf (see Table 1 for the most prevalent root parent tracking companies and their subsidiaries).
[55] See Digital Context Next, Google Data Collection NEW, August 2018, https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.
[56] Ibid.
[57] Response to the CMA's online platforms and digital advertising market study, 29 July 2019, https://privacyinternational.org/advocacy/3101/response-cmas-online-platforms-and-digital-advertising-market-study.

In addition, research by PI shows that cheap smartphones come with a hidden cost: pre-installed apps that can't be deleted and that leak users' data.[58] PI underlined that Android Partners - who use the Android trademark and branding - are manufacturing devices that contain pre-installed apps that cannot be deleted (often known as "bloatware"), which can leave users vulnerable to their data being collected, shared and exposed without their knowledge or consent. We are concerned that this leaves users vulnerable to the exploitative business practices of cheap smartphone manufacturers around the world and have asked Google to make small, reasonable changes that would significantly protect hundreds of thousands of people around the world.[59] This is yet another example of Google's established dominance, in this case as a gatekeeper with the power to improve certified partner devices.

A further concern is transparency and the extent to which consumers will be made aware in a meaningful way of the data implications of the proposed acquisition, both now and in the future. Google and the wider advertising market's track record when it comes to transparency raises numerous questions.

In its Update report into ad-tech and real time bidding, the ICO noted that "*the privacy notices provided to individuals lack clarity and do not give them full visibility of what happens to their data.*"[60] The ICO also underlined that "*the scale of the creation and sharing of personal data profiles in RTB appears disproportionate, intrusive and unfair, particularly when in many cases data subjects are unaware that this processing is taking place.*"[61]

PI raised similar concerns in its submission before the ICO on ad-tech companies and data brokers.[62] PI's submissions demonstrated that many companies fail to comply with basic data protection principles and even seem to work under the assumption that derived, inferred and predicted data and demographic segments do not count as personal data, even if they are linked to unique identifiers or used to target individuals.[63] The lack of transparency is exacerbated by the fact that these companies are non-consumer facing, most people have never heard of these companies, and, even if they have, there is a dearth of information as to

[58] PI, Buying a smart phone on the cheap? Privacy might be the price you have to pay, 20 September 2019, https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay.
[59] PI, We're telling Google: privacy shouldn't be a luxury, 8 January 2020, https://privacyinternational.org/news-analysis/3325/were-telling-google-privacy-shouldnt-be-luxury.
[60] Information Commissioner's Office (ICO), Update report into adtech and real time bidding, June 20, 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.
[61] Ibid.
[62] PI, Our complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad, 8 November 2018, https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad.
[63] PI, Why we've filed complaints against companies that most people have never heard of – and what needs to happen next, 8 November 2018, https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what.

where the data is sourced and who it is shared with. Accordingly, this has a knock-on effect on the exercise of rights and the ability to exercise any control, for example through an access or erasure request. Difficulties faced by members of PI's team in exercising access request rights are set out in the complaints as well as challenges with opt-out mechanisms, there were further frustrations with follow up erasure requests.[64] There was also a lack of willingness to provide Data Protection Impact Assessments and Legitimate Interest Assessments which would provide further insight into companies' justifications for processing and how the rights of individuals have been taken into consideration.

The lack of transparency around the exploitation of users' personal data by online platforms has also negatively impacted the online trust of consumers. According to a 2019 Special Eurobarometer Survey, the majority of respondents indicated that they have partial control over the information they provide online, with 62% of them being concerned.[65] Concerns were also expressed by users in the CMA's report into the collection and use of consumer data. The report found that consumers were concerned about the potential misuse of their data, while they unable to fully understand the precise data companies collected on them and how this data was used exactly.[66]

A combination of Google's extensive and growing databases, user profiles and dominant tracking capabilities with Fitbit's wide-ranging and uniquely sensitive health data could have pervasive effects on individuals' privacy, dignity and equal treatment across their online and offline existence in future.[67] The merger will inevitably reduce what little pressure there currently is on Google to compete in relation to privacy protections available to consumers. This consumer harm flowing from the merger - albeit measured in degraded privacy protections rather than increased prices - is a parameter of competition that is within the ACCC's remit to consider. PI therefore urges the ACCC to consider the serious implications the proposed acquisition will have for consumers privacy as well as their well-being in general, and err on the side of caution in favouring the fundamental freedoms of the many over the financial profits of the few.

Effects on markets/competitors

[64] PI, Have companies deleted your data?, 18 December 2018, https://privacyinternational.org/blog/2549/have-companies-deleted-your-data.
[65] European Commission, Data Protection Regulation one year on: 73% of Europeans have heard of at least one of their rights, 13 June 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2956.
[66] CMA, Commercial use of consumer data, 27 January 2015, https://www.gov.uk/cma-cases/commercial-use-of-consumer-data.
[67] PI, Google wants to acquire Fitbit, and we shouldn't let it!, 13 November 2019, https://privacyinternational.org/node/3276.

At the market level, it has become equally impossible to map, monitor and audit how data flows in an increasingly opaque data ecosystem[68] and some legislative initiatives have emerged seeking to provide more transparency and control over data brokers.[69] However, this is in a context where there is no comprehensive data protection legislation. Yet, whilst data protection law mandates transparency requirements for individual data controllers, including providing information as to the source of personal data and the categories of recipients of personal data, it does not provide for transparency of a particular market, including the digital advertising market.

An example of the impact a digital monopoly can have on both consumers and businesses would be when search engines provide services to third parties that require content indexation capabilities.[70] New or existing search engines must sign 'syndication contracts' to purchase content indexation and content ranking. In exchange, the purchasing company then displays the relevant content, accompanied by ads. As a result, dominant companies monopolising the content indexation market could "force" competitors that rely on their search results to include, for instance, unique identifiers in the URL of the ads that they place. This can seriously undermine the privacy protections offered by these companies to their users as they are then obliged to uniquely identify users, enabling tracking for the providing company, even if they as a company do not collect or retain that data.

In 2015, the Wall Street Journal published a Federal Trade Commission report relating to an investigation into Google's search and advertising practices.[71] The Report notes that "*Google has tied up a substantial portion of this distribution channel with exclusive and restrictive agreements. In the market for search syndication, Google has exclusive or restrictive agreements with 12 of the top 20 companies (60 percent) and 4 of the top 5 (80 percent).*"[72]

Between the demand and supply side of digital advertising are a number of intermediaries, whose role is both to enhance and enrich users' data, and to offer technologies permitting programmatic advertising. These actors rely on data collected through various means and participate in the sharing of personal data at a large scale, through processes such as real time bidding (RTB). What online platforms have in common is their ability to monetise users'

[68] See PI, Corporate Profile Timelines: Google, https://privacyinternational.org/corporateabusetimeline?tid=442.
[69] See, for example, Vermont's Data Broker Regulatory Regime, enacted on May 22, 2018, https://legislature.vermont.gov/assets/Documents/2018/Docs/BILLS/H-0764/H-0764%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf
[70] See, for example, Microsoft, Syndicated Partner Network, https://about.ads.microsoft.com/en-gb/resources/training/syndicated-partner-network.
[71] Wall Street Journal, The FTC Report on Google's Business Practices, 24 March 2015, https://graphics.wsj.com/google-ftc-report.
[72] Ibid, page 104.

attention to sell advertising, while at the same time the more user data they have the more targeted digital ads can be.

It is worth re-emphasising that the amount of user data collected by Google is vast. This includes data when consumers are not signed into a Google Account but is collected with unique identifiers tied to the browser, application or even device an individual is using.

As Google itself sets out, the data goes way beyond what users provide and can include information about apps, browsers and devices; activity in Google services such as terms searched for, videos watched, views and interaction with content and ads, purchase activity, people with whom individuals communicate or share content, activity on third-party sites and apps using Google services and browsing history; as well as location information, determined by GPS, IP address, sensor data, information about things near devices such as Wi-FI access points, cell towers and Bluetooth enabled devices.[73]

The extent that users' personal data might be shared within the online demand-supply chain for the purposes of targeted advertising remains opaque. These transparency concerns were also highlighted by the ICO update report. According to the ICO, "*it is unclear whether RTB participants have fully established what data needs to be processed in order to achieve the intended outcome of targeted advertising to individuals. The complex nature of the ecosystem means that in our view participants are engaging with it without fully understanding the privacy and ethical issues involved.*"[74] The RTB system does not operate in a complete vacuum, rather according to industry frameworks, namely the IAB Europe (Transparency and Consent Framework) and Google (Authorised Buyers Guideline). Various concerns with these frameworks have been raised in a complaint to the ICO and are echoed in similar complaints around the EU.[75]

Large platforms often occupy different positions in the complex online advertising ecosystem.[76] This consequently raises a series of concerns relating to the conflict of interest faced by these platforms, which for example may be a data source, an advertiser and a publisher amongst other roles. A report commissioned by the Department for Digital, Culture,

[73] Google, Privacy Policy, Effective 15 October 2019, https://policies.google.com/privacy?fg=1#infocollect.
[74] Information Commissioner's Office (ICO), Update report into adtech and real time bidding, 20 June 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.
[75] Fix Adtech, https://fixad.tech.
[76] See, for example, Claire Ballentine, Google-Facebook Dominance Hurts Ad Tech Firms, Speeding Consolidation, The New York Times, 12 August 2018, https://www.nytimes.com/2018/08/12/technology/google-facebook-dominance-hurts-ad-tech-firms-speeding-consolidation.html; Mark Sweney, Internet advertising to grow at slowest rate since 2001 dotcom bust, The Guardian, 22 July 2019 https://www.theguardian.com/media/2019/jul/22/internet-advertising-grow-digital-scandals-facebook-google.

Media & Sport on online advertising in the UK highlighted that, as a consequence of their ownership of also strong user data assets, "*Google and Facebook are, to some extent, able to set their own terms to advertisers and publishers*."[77]

PI believes that the proposed acquisition would have the effect, or be likely to have the effect of substantially lessening competition in -at least- the general search market and the digital advertising market by granting Google even more dominance and thus allowing it to engage in anti-competitive behaviour, by, for instance, imposing unprecedent barriers for competitors to enter these markets, or being able to significantly and sustainably increase prices or profit margins, ultimately harming innovation and competition.

The unavailability of remedies to effectively prevent the substantial lessening of competition requires the proposed acquisition be forbidden

Google has a long track record of competition law infringements in the EU, including violations of competition on the search market,[78] on Google Play Store and Android[79] and on the market for online advertising intermediation.[80] The company is also currently under investigation in the United States[81] as well as by the ACCC for its conduct in relation to location data.[82]

In January 2019, the French data protection authority (CNIL) fined Google a record 50 million euro fine for "failing to provide users with transparent and understandable information on its data use policies".[83] The CNIL decision pointed out that the violations were aggravated by the fact that Google's economic model "is partly based on ads personalisation", and that it was therefore "its utmost responsibility to comply" with GDPR.[84]

---

[77] Stephen Adshead, Grant Forsyth, Sam Wood, Laura Wilkinson, Online advertising in the UK, A report commissioned by the Department for Digital, Culture, Media & Sport, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777996/Plum_DCMS_Online_Advertising_in_the_UK.pdf.

[78] Official Journal of the European Union, Summary of Commission decision of 27 June 2017 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case AT.39740 — Google Search (Shopping)) (notified under document number C(2017) 4444) (2018/C 9/08), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1516198535804&uri=CELEX:52018XC0112(01).

[79] European Commission, Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine, 18 July 2018, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581.

[80] European Commission, Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising, 20 March 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.

[81] FT, Which antitrust investigations should Big Tech worry about?, https://www.ft.com/content/abcc5070-f68f-11e9-a79c-bc9acae3b654.

[82] ACCC, Google allegedly misled consumers on collection and use of location data, 29 October 2019, https://www.accc.gov.au/media-release/google-allegedly-misled-consumers-on-collection-and-use-of-location-data.

[83] Alex Hern, Google fined record £44m by French data protection watchdog, The Guardian, 21 January 2019, https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog.

[84] CNIL, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

Taking into account Google's privacy and competition past, PI urges extreme caution when it comes to potential remedies considered by the ACCC, during the investigation of the proposed acquisition. Such remedies must not risk proving ineffective in the long run or seriously impair consumers' fundamental freedoms. Specifically, PI is deeply concerned about suggestions or potential remedies involving data sharing (access to data by competitors), anonymisation techniques and data silos, for the following reasons.

First, personal data is not just any other economic asset. Privacy and the protection of personal data are fundamental human rights. As both the UK CMA[85] and the ICO[86] have acknowledged, the way in which several players currently collect, amass and generate data often lacks transparency and seeks to maximise the amount of data available, through unfair means. This creates a race to the bottom; these dominant players already hold vast amounts of personal data across multiple services, and, even then, they still seem to be in a constant mission for more.[87] Data enhances their dominant position and exploitation –the lack of transparency, the manner in which such data is collected and then used, are all points which need addressing. This is why modern data protection laws like the EU General Data Protection Regulation include principles such as transparency, fairness, data minimisation and purpose limitation, and recognise the right to data portability, and demand that individuals must be given the tools to be in control of their data. PI is very concerned that the implementation of personal data sharing standards can pose grave risks also for the security and integrity of consumers' personal data.[88]

Second, there is a fine line between pseudoanonymous and anonymised data. The first can still render an individual identifiable. For example, journalists from the German public broadcaster NDR were able to identify the sexual preference and medical history of judges and politicians, using online identifiers.[89] This is just one example, that serves to illustrate the insights that can be gleaned from seemingly mundane and pseudonymous data and the

[85] Competition and Markets Authority (CMA), Online platforms and digital advertising, Market study interim report, December 2019.
[86] Information Commissioner's Office (ICO), Update report into AdTech and real time bidding, 20 June 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.
[87] PI, Competition and Data, 26 September 2018, https://privacyinternational.org/explainer/2293/competition-and-data.
[88] On 11 July 2019, the Irish Data Protection Commission (DPC) received a data breach notification from Google, following reports that contractors could listen to recordings made from people's conversations with their Google Assistant, see Stephanie Bodoni, Google Data Breach Faces Review by Irish Privacy Watchdog, Bloomberg, 12 July 2019, https://www.bloomberg.com/news/articles/2019-07-12/google-data-breach-faces-review-by-irish-privacy-watchdog.
[89] Alexander Martin, Browsers nix add-on after Web of Trust is caught selling users' browsing histories, The Register, 7 November 2016, https://www.theregister.co.uk/2016/11/07/browsers_ban_web_of_trust_addon_after_biz_is_caught_selling_its_users_browsing_histories.

value it might have.[90] Even if it is not a company's intention to directly identify an individual, this is still possible, due to the vast amount of data it might collect and generate. And, even when data seem to be truly anonymised by companies, and consequently exempt from the protection guaranteed by the General Data Protection Regulation, for example, this anonymisation might still lead to the re-identification of individuals.

In 2015, researchers at Harvard University found vulnerabilities in the anonymisation procedures used for health care data in South Korea that enabled them to de-anonymise patients with a 100% success rate and to decrypt the Resident Registration Numbers included with prescription data relating to deceased South Koreans. The unique 13-digit codes enabled full reidentification. In the UK, medical information is held on the NHS Personal Demographics Service is identified by the patient's ten-digit NHS number. In the UK, Cambridge University security engineer Ross Anderson noted that the problem is that 800,000 NHS employees need access to the PDS; Hampshire GP Neil Bhatia agreed that the large number of users means that access can't be audited or controlled and relies on trust.[91] Similarly, in a more recent study, researchers were able to demonstrate that, despite the anonymisation techniques applied, "*data can often be reverse engineered using machine learning to re-identify individuals*."[92]

Third, in their press releases surrounding the merger both Google and Fitbit assure users that no personal data will be exploited as a result of this acquisition. Specifically, both Fitbit and Google underline that "Fitbit health and wellness data will not be used for Google ads",[93] while Google further adds that Fitbit users will be given "the choice to review, move, or delete their data".[94]

In the past similar statements have been made to the European Commission in relation to mergers that have resulted in pervasive and problematic data sharing schemes between the merging entities. Two examples are the Google / DoubleClick merger[95] and the Facebook /

[90] See PI, Corporate Profile Timelines: Google, https://privacyinternational.org/corporateabusetimeline?tid=442.
[91] Alexander Martin, Has somebody shared your 'anonymised' health data? Bad news, The Register, 2 October 2015, https://www.theregister.co.uk/2015/10/02/s_korean_anonymised_health_data_sharing_a_breach_in_waiting.
[92] Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de Montjoye, Estimating the success of re-identifications in incomplete datasets using generative models, *Nature Communications* volume 10, Article number: 3069 (2019), https://www.nature.com/articles/s41467-019-10933-3.
[93] Fitbit, Fitbit to Be Acquired by Google, 1 November 2019, https://investor.fitbit.com/press/press-releases/press-release-details/2019/Fitbit-to-Be-Acquired-by-Google/default.aspx; Rick Osterloh, Helping more people with wearables: Google to acquire Fitbit, Google, 1 November 2019, https://blog.google/products/hardware/agreement-with-fitbit.
[94] Rick Osterloh, Helping more people with wearables: Google to acquire Fitbit, Google, 1 November 2019, https://blog.google/products/hardware/agreement-with-fitbit.
[95] Case No COMP/M.4731 – Google/ DoubleClick, Commission decision of 11/03/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement, C(2008) 927 final, 11 March 2008, https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf.

WhatsApp merger,[96] which led to a number of decisions finding that the parties had misled competition regulators.[97]

DoubleClick was one of the first companies set up to sell display advertising on the web. Set up in 1996, it went public in 1998, and in 1999 merged with the data collection company Abacus Direct. In response to a 2001 US Federal Trade Commission investigation of the proposed merger, DoubleClick promised to keep those two databases separate; and in 2005 when the private equity firm Hellman & Friedman acquired it, that firm promised to operate the company as two separate divisions. In April 2007, Google acquired DoubleClick for $3.1 billion in cash. The merger was approved by both the EU's regulators and the FTC on the basis that it was unlikely to lessen competition even though by then Google had become dominant in pay-per-click internet advertising.[98] The FTC held that privacy issues were not relevant to an antitrust review. At the acquisition, Google founder Sergey Brin said privacy would be the company's "number one priority" when considering new advertising products.

In the summer of 2016, it was reported that Google erased the line in its privacy policy that promised to keep DoubleClick's database of web browsing records separate from the names and personally identifiable information Google collects from Gmail and other login accounts.[99] PI is deeply concerned that history will once again repeat itself. As the ACCC chairman Rod Sims stated at the Consumer Policy Research Conference in Melbourne in November 2019, referring to Google's promise not to combine DoubleClick's advertising data with Google search data, it "is a stretch to believe that commitment will still be in place five years from now".[100]

The proposed acquisition should not go ahead without strong and future-proof safeguards. However, for the reasons set out above, including Google's already dominant position and history and the highly sensitive nature of Fitbit's data, we are unconvinced that this is possible.

Conclusion

[96] Case M.7217 – Facebook/ WhatsApp, Commission decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004, C(2014) 7239 final, 3 October 2014, https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf.
[97] European Commission, Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover, 18 May 2017, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369.
[98] Diane Bartz, Google wins antitrust OK to buy DoubleClick, Reuters, 20 December 2007, https://www.reuters.com/article/us-doubleclick-google/google-wins-antitrust-ok-to-buy-doubleclick-idUSN2039512220071220.
[99] Julia Angwin, Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking, ProPublica, 21 October 2016, https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking.
[100] John Davidson, Will Google mine your Fitbit data? The ACCC thinks so, Financial Review, 19 November 2019, https://www.afr.com/technology/google-will-mine-fitbit-data-for-advertising-accc-warns-20191119-p53bxy.

In light of the considerations outlined in this submission, PI considers that the proposed acquisition would have the effect, or be likely to have the effect, of substantially lessening competition, by harming both consumers and other business or competitors in at least the general search market and the digital advertising market, in which Google already has a concentration of market power, as well as in the health-related and/or insurance markets, into which Google is planning to enter.

We therefore ask the ACCC to prohibit the proposed acquisition in accordance with its powers under section 50 section of the Competition and Consumer Act 2010. In the alternative, and as a minimum we ask that the ACCC impose strong and future-proof safeguards. Any such safeguards would require further consideration, but options for considerations include data silos and independent regulatory scrutiny.

We would be pleased to engage further with the ACCC on any aspect of this submission, including providing further information on any of the issues referred to above.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).