Response to the Australian Competition and Consumer Commission's Statement of Issues: Proposed acquisition of Fitbit, Inc. by Google LLC

July 2020

privacyinternational.org

9 July 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 response to the ACCC's Statement of Issues - Google LLC – proposed acquisition of Fitbit Inc

Introduction

Privacy International ("PI") welcomes the Australian Competition and Consumer Commission's (the "ACCC") request for submissions in response to its Statement of Issues ("SOI") dated 18 June 2020 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 companies and governments who exploit individuals' data and technologies. PI employs specialists in their fields, including technologists and lawyers, to understand the impact of existing and emerging technology upon data exploitation and our right to privacy, including in relation to online platforms and the advertising technology ("ad tech") industry.

PI has an established track record of engaging with competition regulators around the world on issues that concern the intersection of data/privacy and competition laws. For example, we have submitted evidence to the European Commission,[1] the UK Competition and Markets

[1] PI, Privacy International's submission to the European Commission consultation on 'shaping competition policy in the era of digitisation', 2 October 2018.

Authority (CMA)[2] and the U.S. Federal Trade Commission (the FTC)[3] regarding data and competition issues.

PI broadly welcomes the ACCC's outline of its preliminary concerns in the SOI, several of which correspond with the points raised in our March 2020 submission to the ACCC in relation to the proposed acquisition. The present submission further elaborates on some of those points and also seeks to provide PI's views on some of the other issues of concern identified in the SOI.

Specifically, we first wish to underline the importance of examining Google's wealth of consumer data pre- and post-transaction, as an integral part of the ACCC's assessment of the competitive effects of the proposed acquisition. Second, we illustrate the wealth of Fitbit's data which can further augment Google's dominance in the digital advertising market, as well as allow Google further market power in the market for data-dependent health services, including by eliminating competition between Google and Fitbit in this increasingly important market and raising barriers to entry, with negative consequences for consumers. Third, we argue that the proposed acquisition is likely to lead to the foreclosure of competitors to Google in the growing wearables market and therefore result in a lessening of competition in the aforementioned market.

Finally, we respectfully ask the ACCC to apply very close and strict scrutiny in its review of the proposed acquisition. PI is concerned that the potentially harmful effects of the transaction cannot, in this case, be addressed by accepting remedies, especially remedies such as third-party data access or data sharing practices, which might seriously underline consumers' privacy and data protection rights.

I. The importance of examining Google's wealth of consumer data pre- and post-transaction

Individuals' data is the most important asset in the digital economy. The acquisition of vast quantities of data is what allows companies like Google to make billions of dollars each year via targeted advertising. In 2019 for example, Google's parent company, Alphabet, generated 83% of its $161.86 billion in revenue from delivering targeted advertisements to the

[2] PI, Submission to the Competition and Markets Authority's call for information on digital mergers, 23 July 2019; Response to the CMA's online platforms and digital advertising market study, 29 July 2019.
[3] PI, Submission to the US Federal Trade Commission on the intersection between privacy, big data, and competition, 1 August 2018.

users of their many consumer-facing services, which include the Android operating system, Google Search, YouTube, Gmail, and many others.[4]

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.[5] With the development and integration of artificial intelligence (AI) technologies, it is likely that users' data will become even more important for these companies, since such data is an essential input to train AI models. [6]

As huge concentrations of power arising from the value of data in the digital economy already exist, it is of utmost importance that Google's data holding is central to the ACCC's competitive assessment of the proposed transaction. Indeed, the importance of data holding is very well-recognised by the tech giants, like Google, who consistently regard consumers' data as a business asset.[7] Data is also absolutely integral to these companies' business models and therefore their market value.[8] We note as above 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.[9]

PI welcomes the ACCC's preliminary view that the "*accumulation of additional, individual user data via this transaction in an entity which already benefits from substantial market power in multiple markets may contribute to reduced competitive outcomes in the future*".[10] As the SOI states:

> "*Google currently has more avenues from which to gather consumer data than any other company and this gives it a significant competitive advantage in many markets.*

[4] 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, 2019).
[5] Maurice Stucke and Allen Grunes, *Big Data and Competition Policy*, 2016 Oxford University Press.
[6] In case AT.39740 *Google Shopping* the European Commission considered barriers to entry and expansion in general search and noted the response of one company that underlined the importance of data and AI in this market: *"obtaining the large quantity of data necessary to develop an effective [general] search engine (e.g., the information upon which relevancy algorithms can be built and improved) would be a significant barrier to entry"* (recital 286).
[7] European Data Protection Supervisor (EDPS), Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 September 2016.
[8] The CMA note in its final report on its market study into online platforms and digital advertising dated 2 July 2020 (CMA Final Report) (at para 4.2) that *"While platforms provide services that are free to consumers when they use them, some also generate very large revenues – and are extremely profitable. Their business model relies on attracting consumers' attention and gathering data about them, which they use to sell personalised advertising."*
[9] We note that paragraphs 2.18 and 2.19 of the CMA Final Report detail the types of data which Google is able to combine to calculate consumer preferences and purchasing intent.
[10] ACCC, Statement of Issues: Google LLC – proposed acquisition of Fitbit Inc. (18 June 2020), para 6.

The health and fitness data collected by Fitbit will provide Google with access to consumer data that is likely to be an important element of services in several markets."[11]

The ability to deal appropriately with concentrations of data is therefore key to evolving competition rules to deal with the challenges and realities of the digital economy. An assessment as to a company's data holding pre- and post-transaction is highly relevant to the competitive effects of the transaction: it is not solely a matter for data protection regulators. It must, therefore, be considered by competition regulators in any competitive assessment of mergers in this sector.

As Professor Tommaso Valletti noted before the US House of Representatives Judiciary Committee Subcommittee on Antitrust, Commercial, and Administrative Law in October 2019, privacy is at the heart of the economics of the digital platforms and competition is shaped around it. It follows that where there is little competition, quality is degraded, particularly through reductions in consumers' privacy. It is absolutely vital that the ACCC consider the impact on competition for data privacy when considering the proposed acquisition. Were it to do so, in PI's view, the ACCC would conclude that the concentration will cause a significant impediment to effective competition.

II. The wealth of Fitbit's data can augment Google's dominance in the digital advertising market, as well as allow Google further market power in the market for data-dependent health services

As the ACCC rightly notes, the data possessed by Fitbit "*is voluminous in depth and the nature of its customer base is such that it lends itself to having value for drawing health insights or for developing data-dependent health services*".[12]

The analysis below seeks to demonstrate the extent of Fitbit's data collection practices, which often involve the processing of sensitive personal data. Should Fitbit's acquisition by Google be permitted, then some or all of the data categories mentioned below might be potentially integrated into or used to further strengthen Google's dominant position in the digital advertising or health-related markets.

Fitbit data analysis

[11] Ibid, para 13.
[12] ACCC, Statement of Issues: Google LLC – proposed acquisition of Fitbit Inc. (18 June 2020), para 10.

This analysis is predominantly based on Fitbit's Privacy Policy (effective: 18 December 2019).[13] It is further supplemented by screenshots, which aim to illustrate the various types of personal data that might be processed while using the Fitbit. The screenshots were captured between February and March 2020, as part of an exercise carried out by PI staff, which involved the occasional use of a Fitbit "Charge 3" device[14] and its association with PI staff personal smartphone(s), together with a Fitbit premium subscription.[15]

1. Categories of personal data obtained by Fitbit

1.1. Personal data obtained directly from Fitbit users

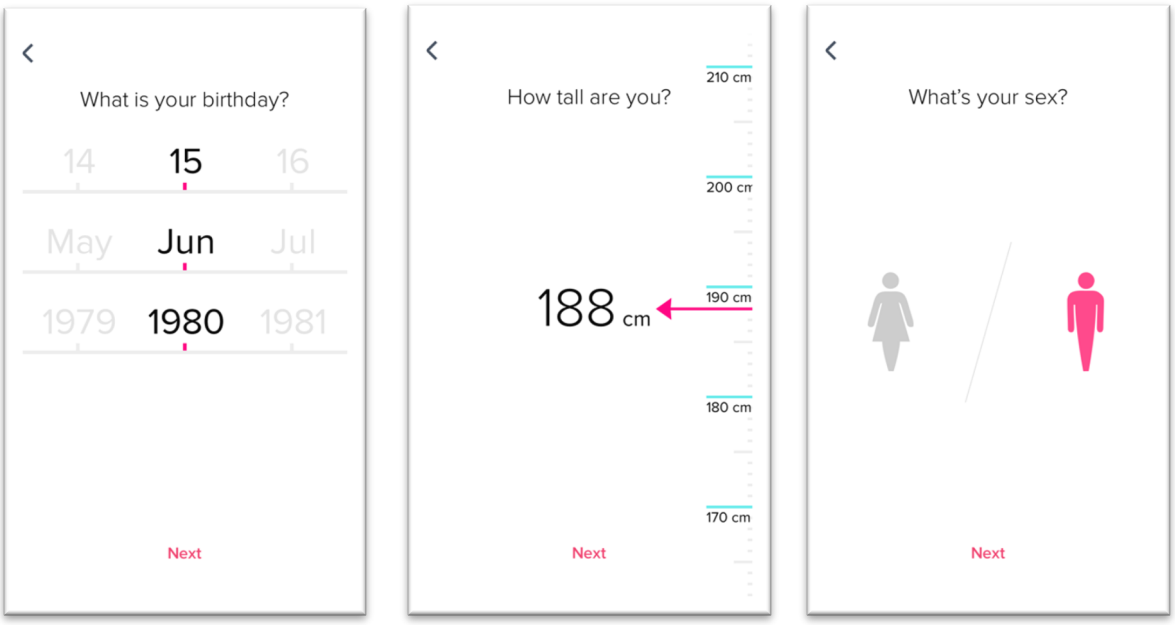
a. Biographical data etc.

According to the Fitbit Privacy Policy, the following information is collected from users while setting up their account:

> *"name, email address, password, date of birth, gender, height, weight, and in some cases your mobile telephone number. This is the only information you have to provide to create an account with us. You may also choose to provide other types of information, such as a profile photo, biography, country information and community username*."

The screenshots below illustrate how this data collection takes place while users sign up to the Fitbit services via the Fitbit app.

[13] Fitbit, Fitbit Privacy Policy (effective: 18 December 2019). Any references to the terms Fitbit or Fitbit services should be deemed to mean Fitbit, Inc. as well as its devices, applications, software, websites, APIs, products, and services.
[14] Fitbit Charge 3 product page on Fitbit's website.
[15] Fitbit, fitbit premium.

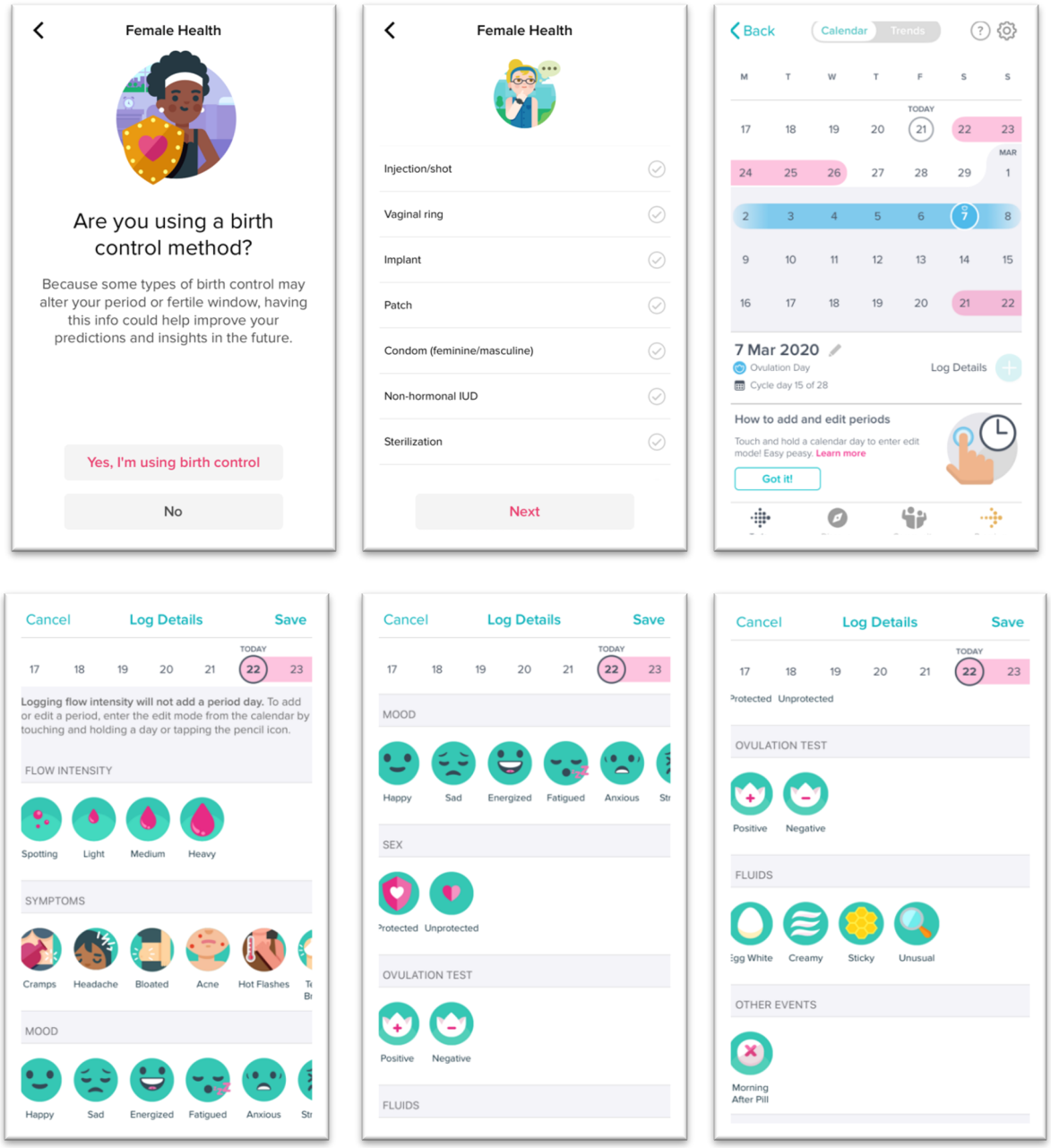


b. Sensitive data regarding individuals' health, sex life etc

According to the Fitbit Privacy Policy, Fitbit additionally collects the following categories of personal data that users might choose to provide:

> "*To help improve your experience or enable certain features of the Services, you may choose to provide us with additional information, like your logs for food, weight, sleep, water or female health tracking; an alarm; and messages on discussion boards or to your friends on the Services.*"

The following screenshots illustrate how the collection of the aforementioned data takes place within the Fitbit app. As the screenshots show, this may also include sensitive data not only in relation to health data but also with regard to other sensitive data, such as data concerning a person's sex life or sexual orientation. For example, 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.



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

c. Data about individuals' contacts

Users may also choose to connect with other users that use the Fitbit app or invite others to join the Fitbit services "*by providing their email addresses, accessing social networking accounts, or using the contact list on your mobile device*". This accordingly means that, where a user decides to provide personal data of other individuals, by logging into their social media accounts via Fitbit or granting Fitbit access to their contact list on their mobile device, then Fitbit will consequently process the personal data of these other individuals.

Additionally, according to the Fitbit Privacy Policy:

"*If you contact us or participate in a survey, contest, or promotion, we collect the information you submit such as your name, contact information, and message.*"

d. Payment and card data

Some Fitbit fitness tracker models/devices can facilitate payments and transactions with third parties, for example, by allowing users to pay in a similar fashion that they would make payments or transactions using contactless payment features on their mobile phones. According to the Fitbit Privacy Policy:

"*If you activate this feature, you must provide certain information for identification and verification, such as your name, credit, debit or other card number, card expiration date, and CVV code. This information is encrypted and sent to your card network, which upon approval sends back to your device a token, which is a set of random digits for engaging in transactions without exposing your card number. For your convenience, we store the last four digits of your card number and your card issuer's name and contact information. You can remove the token from your account using your account settings. We do not store your transaction history.*"

In relation to purchases made on the Fitbit website, the Fitbit Privacy Policy reads:

"*If you purchase Fitbit merchandise on our website, you provide your payment information, including your name, credit or debit card number, card expiration date, CVV code and billing address. We do not store this payment information. We store your delivery address to fulfil your order.*"

e. Data from the use of Live Coaching Services

Finally, users might use Fitbit Coach[16], Fitbit's live coaching services, a platform that according to Fitbit's Privacy Policy enables users "*to communicate with a live health, fitness or wellness coach*". The Privacy Policy states:

"*Coaches may be provided by third parties, such as your employer or insurance company, or by our third-party coaching service providers. If you use our Live Coaching Services, we collect information about such use, including the plan, 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.*"

[16] https://coach.fitbit.com

1.2. Personal data obtained through the use of the Fitbit services

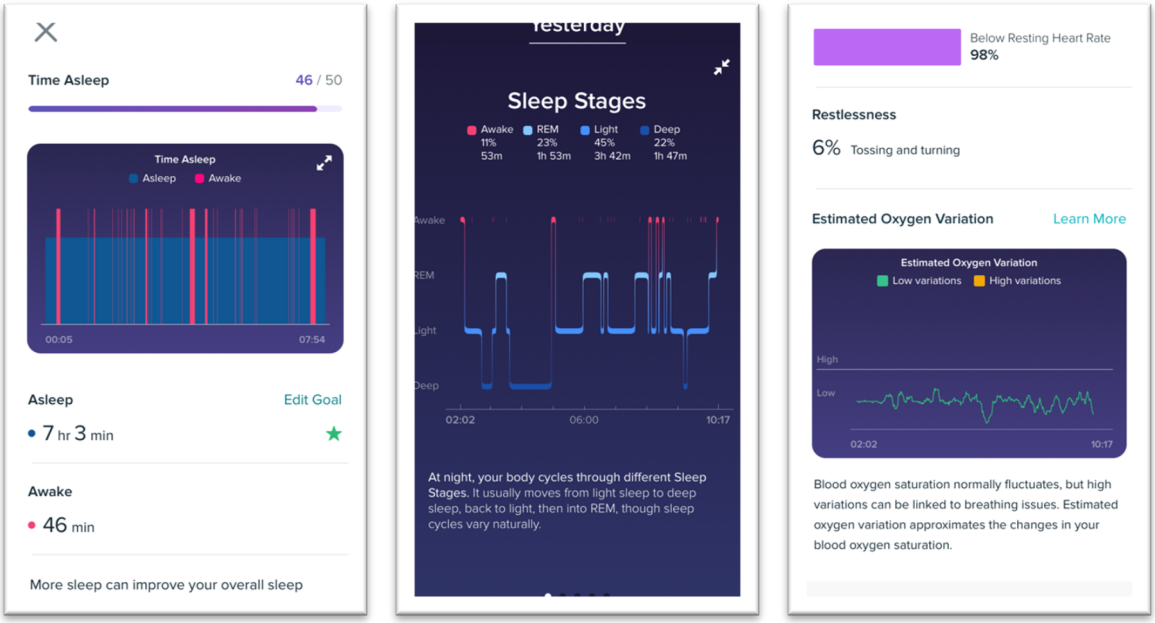
Based on their Privacy Policy, Fitbit collects the following categories of personal data indirectly or from the use of the services without users directly providing this personal data to the Fitbit services. In this case, the data collection takes place mainly via the user's device and, as illustrated below, it can be extremely intrusive.

The personal data that Fitbit services obtains from individuals' use of their services and not from them directly can be split into three categories: (i) Personal data collected by Fitbit devices; (ii) Geolocation data; and (iii) usage or network activity data. The Fitbit Privacy Policy does not provide an exhaustive list, as indicated by the emphasis in the following extracts: "*data to estimate a variety of metrics **like***" for data collected by Fitbit devices; "***include** features that use precise geolocation data, **including***" for geolocation data of users; and "***includes** information*" for usage or network activity data). However, the table below provides an overview of the categories of personal data collected within the ambit of these three wider categories.

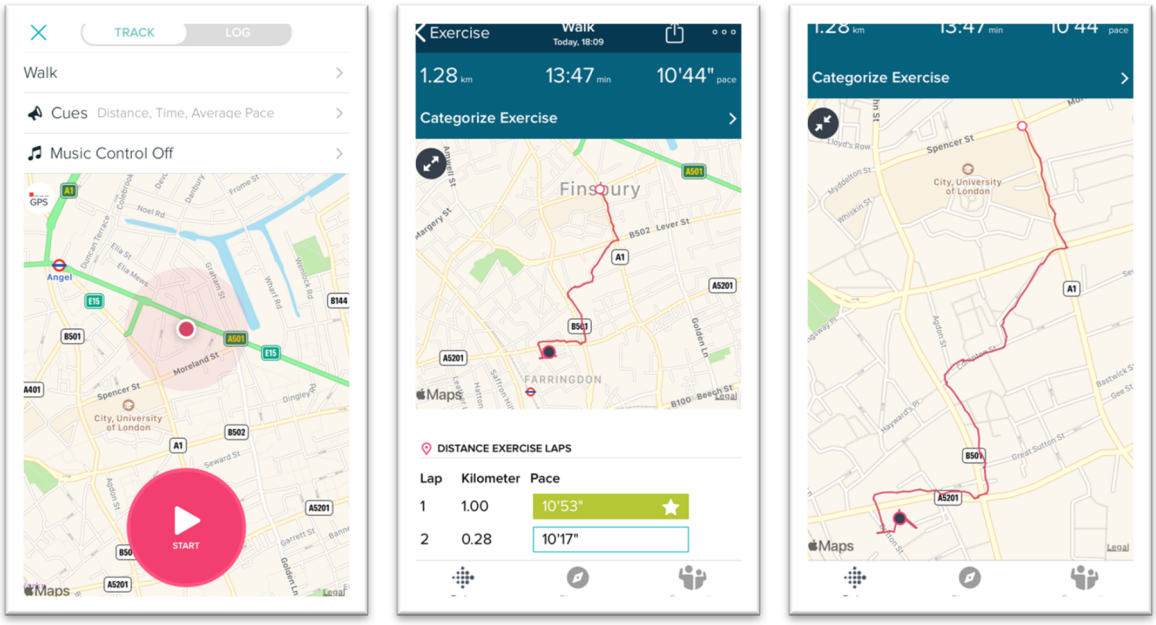
Data collected by Fitbit devices	Number of steps, distance travelled, calories burned, weight, heart rate, sleep stages, active minutes and location.
Geolocation data	GPS signals, device sensors, Wi-Fi access points, and mobile mast IDs, approximate location based on IP address.
Usage or network activity information	Information about individuals' interactions with the Fitbit services; viewing or searching content; installing applications or software; creating or logging into an account; pairing devices to accounts; opening or interacting with applications on Fitbit devices; data about the devices and computers used to access the Fitbit services, such as IP addresses, browser type, language, operating system, Fitbit or mobile device information (including device and application identifiers), the referring web page, pages visited, location, and cookie information.

The screenshots below seek to complement some of the categories of personal data mentioned in the table above, highlighting the extent of Fitbit's data collection and the sensitive nature of the personal data that Fitbit service might obtain.

Data collected by Fitbit devices and sensors: *Examples of heart rate data collected by Fitbit devices and the relevant inferences they may result in such as how fit you are.*



Data collected by Fitbit devices and sensors: *Example of data relating to sleep stages and the relevant inferences they may result in, including your level of restlessness and potential breathing issues.*



Geolocation data: *Examples of GPS tracking data collected by Fitbit.*

1.3. Personal data obtained via third parties

Finally, Fitbit might obtain personal data of users via third parties. For example, as set out in the Fitbit Privacy Policy, if users connect to Facebook or Google, Fitbit may receive personal data such as individuals' names, profile pictures, age range, languages, email addresses, and friend lists. Similarly, if users link their exercise or activity data held on another service to Fitbit, then the latter can obtain access these data.

Furthermore, Fitbit may also receive personal data from third parties such as employers or insurance companies. The Privacy Policy states:

> "*We may partner with third parties, such as employers and insurance companies that offer Fitbit Services to their employees and customers. In such cases, those companies may provide us with your name, email address or similar information (like a telephone number or subscriber ID) so that we can invite you to participate or determine your eligibility for particular benefits, such as discounts or free services.*"

1.4. Complete list of categories of personal data obtained by Fitbit

The table below illustrates the extent of the personal data that Fitbit services might collect based on the category of personal data. As mentioned above, these personal data might be provided directly by users; be collected via users' devices or while they use the Fitbit services,

including Fitbit's live coaching services; or third parties such as services users link their Fitbit account to, or their employer or insurance company.

Data Category	Examples of personal data
User identifiers' data	Name or username, email address, postal address, phone number, IP address, account ID, device ID, cookie ID, and other similar identifiers.
Demographic data	Gender, age, health information, and physical characteristics or description; biography or country.
Commercial data	Payment information and records of the Services or devices purchased, obtained or considered (for example, if they were added to shopping basket on the Fitbit online store but not purchased).
Sensitive or special-category data	Personal data concerning health or a person's sex life or sexual orientation, as well as biometric data may be gathered from the following data: exercise, activity, sleep or health data, including the number of steps, distance travelled, logs for food and calories burned, weight, heart rate, sleep stages, active minutes, female health data such as data about symptoms, contraception and sexual activity, Live Coaching Services data (provided by users or their coach), and any similar information to which a user might grant access from another service.
Internet or other electronic network activity data	Usage data such as information about interactions with the Services and about the devices and computers used to access the Services.
Geolocation data	GPS signals, device sensors, Wi-Fi access points, and mobile mast IDs, if users have granted us access to that information.
Electronic, visual or similar information	Profile photos or other photos.
Professional or employment related information	Information, such as names, email addresses, that employers provide to Fitbit so that Fitbit can invite individuals to participate in or determine individuals' eligibility for Fitbit Services that they offer to their employees.
Other data	Account information such as; information for features of the Services, for example, an alarm; information about friends;

	messages on the Services; and other information recorded by Fitbit devices.
Inferences	These could be drawn from any of the data contained in the rows above, including number of calories burned, distance travelled, sleep insights, and personalised exercise and activity goals and may include sensitive inferences about an individual's health and sex life.

2. Using Fitbit's "unique" and highly sensitive data to augment Google's dominance in the digital advertising market

As shown above, Fitbit collects large amounts of personal data which may include extremely sensitive data, such as data relating to health or concerning a natural person's sex life or sexual orientation.[17] Several of these categories of personal data, such as geolocation, sleep pattern inferences and other profiling may not be collected directly from users, but from their devices, or usage and network activity. Finally, under certain circumstances, Fitbit might receive additional personal data about individuals from their employers or insurance companies. This final point is quite important because, together with the rest of the examples mentioned in this analysis, it underlines the need 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.

As the ACCC understands, "*the health and fitness data collected by Fitbit is likely to be useful in improving certain ad tech services, predominantly by allowing suppliers with existing information on individual online users to better target display advertising to those particular consumers*."[18]

By combining data they already have with sensitive personal data held by Fitbit, Google could potentially enrich their datasets and provide more detailed audience insights and

[17] 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 of the 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.

[18] ACCC, Statement of Issues: Google LLC – proposed acquisition of Fitbit Inc. (18 June 2020), para 18

segmentation that advertisers could use to target consumers on the basis of health conditions, activity levels, emotional attributes etc. At this point, we would like to draw the attention of the ACCC to the UK Information Commissioner's Office (ICO) June 2019 Update report into adtech and real time bidding. The report looks into real time bidding (RTB), an automated process that takes place (when implemented) every time a page with available advertising space is loaded. During this process a wide range of data is broadcasted to multiple advertisers and put to auction.[19]

In the update report, the ICO note:

- the types of information gathered within RTB are governed by particular industry specifications known as protocols, usually, OpenRTB or Google's Authorized Buyers Real Time Bidding Protocol;
- more detailed bid requests are deemed to be more attractive, either because they bring in higher revenue and/or because they are intended to enable more accurate targeting of adverts to individuals; and
- parties within the RTB ecosystem may also 'augment' the data collected with information from other sources, a process known as 'data matching' or 'enrichment'.[20]

For example, Google's 'publisher verticals',[21] contain several fields pertaining, among others, to fitness, physical and mental health, such as "Reproductive Health", "Sex Education & Counseling", "Dating & Personals", "Vitamins & Supplements", "Pharmacy", "Medical Devices & Equipment", "Substance Abuse", "Health Conditions", "Mental Health", "Special & Restricted Diets", "Counseling Services", "Men's Health", "Women's Health", "Fitness Instruction & Personal Training", "Gyms & Health Clubs", "Running & Walking".[22]

The ICO update report underlines:

> "*We have heard assertions that, in some cases, such fields are not used for profiling individuals, but instead for alerting advertisers to the nature of the website being visited by the user, thereby enabling advertisers to prevent their adverts being placed*

[19] PI, "Why am I really seeing that ad? The answer might be Real Time Bidding (RTB)" (21 May 2019).
[20] Information Commissioner's Office (ICO), Update report into AdTech and real time bidding (June 2019).
[21] Google, Protos & Reference data.
[22] See Google's list of publisher verticals.

on unsuitable websites. However, for both protocols, some of the published documentation states that these fields are used for both targeting and exclusion."[23]

Finally, we note that in its final report into online platforms and digital advertising the UK Competition and Markets Authority (CMA) refers to Google's various data collection practices and the fact that, according to advertisers and media agencies, Google seems to provide "*in-depth targeting options, driven by its unique and vast sources of data*".[24]

In the digital advertising/ad tech context, Fitbit data could be used by Google for audience insights and segmentation that advertisers could use to target consumers on the basis of health conditions, activity levels, emotional attributes and potentially even sexual activity. Access to such data would present Google with an even greater competitive advantage, as Google's competitors in digital advertising would not be privy to the same quantity or quality of such data. As a result, the proposed transaction would significantly impede actual/potential competitors' ability to compete with the merged entity in the provision of digital advertising/ad tech services.

3. Using Fitbit's "unique" and highly sensitive data to further market power in the market for data-dependent health services

Fitbit's products and services provide extensive health tracking capabilities. Insofar as digital or data-dependent health services are concerned, Fitbit's data would therefore be extremely valuable to Google post-transaction. The proposed acquisition would afford Google access to data that it could use to further expand in markets for health services, an area which, as the examples below illustrate, is of significant commercial interest to Google. In particular:

- In January 2016, the European Commission was notified of a proposed concentration by which Sanofi SA (Sanofi being a global pharmaceutical group engaged in the research, development, manufacture and marketing of healthcare products) and Google, the latter through its wholly-owned subsidiary Verily Life Sciences LLC, planned to acquire joint control of a newly created company. Verily was established in order to group together Google's life sciences related projects. The joint venture was set up to offer services for the management and treatment of diabetes. In addition, the joint venture sought to commercialise certain products (such as specialised continuous glucose monitoring devices, insulin pumps and insulin) which

[23] Information Commissioner's Office (ICO), Update report into AdTech and real time bidding, June 20, 2019, page 13.
[24] CMA Final Report para 41 ff.

can be used alongside the services.[25] The joint venture was cleared unconditionally in February 2016.[26]

- In October 2018, the European Commission cleared under the Simplified Procedure a new joint venture set up by Google's Verily and ResMed Inc to study the health and financial impacts of undiagnosed and untreated sleep apnea and other breathing related sleep disorders, and develop software solutions that enable health care providers to more efficiently identify, diagnose, treat and manage individuals with sleep apnea and other breathing related sleep disorders.[27]

- Last year it was revealed that Google has partnered with Ascension, the second largest healthcare provider in the US.[28] As part of the so-called "Project Nightingale", Google has supposedly received healthcare information of up to 50 million Americans, including sensitive information such as names and medical history, without anonymisation.[29]

Google and Fitbit are potential competitors in the market for digital or data-dependent health services. Allowing Google to acquire what is currently a competitor in this market will significantly impede effective competition, including by raising barriers to entry as a result of Google's vast data resource, at what might be a critical point for the development of this increasingly important market. Post-transaction, Google would effectively leapfrog competitors and take pole position in terms of the health-related data at its disposal - a critical input for any undertaking to be a serious player in digital or data-dependent health services. PI urges the ACCC to recognise the dangers inherent in allowing Google to acquire such a critical input for this market.

Google's expansions into health markets also raise concerns around the level of privacy it provides in those markets, which for the reasons set out above should be considered as part of the competition assessment insofar as non-price competition is important to consumers. In particular:

---

[25] See: 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.
[26] In its clearance decision (Case M.7813 - Sanofi/Google/DMI JV, 23 February 2016), the European Commission highlighted the possibility of a market for "*algorithms for analysing healthcare data*" (paras 46-48) and the concerns around data portability of a digital e-medicine platform, but noted that the GDPR serves to capture any data protection concerns (paras 68-70).
[27] European Commission, Case M.8991 – Alphabet/ResMed/JV (1 October 2018).
[28] Rob Copeland, Google's 'Project Nightingale' gathers personal health data on millions of Americans, The Wall Street Journal, 11 November 2019.
[29] Ed Pilkington, Google's secret cache of medical data includes names and full details of millions – whistle bower, The Guardian, 12 November 2019.

- In 2015, the Royal Free Hospital 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 (the "**ICO**"), subsequently 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 noted the risk that 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]

It therefore seems likely, based on the above examples, that permitting Google greater power in the markets for data-dependent healthcare services will not encourage greater competition on the basis of privacy in these markets and will likely result in degraded standards of data privacy for consumers of such services.

III. Ability and incentive for Google to foreclose competing wearable manufacturers

Wearable technology acts as both a device for collection of health-related (and often sensitive) data, and as another gateway to the internet. The importance of wearables for the purposes of access to search and to the internet more broadly is growing, as the ACCC rightly note in their SOI:

> *"Current information suggests that wearables are an emerging channel or platform through which many services may be offered and data collected. This is exhibited by the expansion of many technology companies into wearables in recent years. Wearables are likely to be capable of many of the core functions currently undertaken by smartphones, particularly as the use of voice assistants and cellular connectivity*

[30] Hal Hodson, Revealed: Google AI has access to huge haul of NHS patient data, New Scientist, 29 April 2016.
[31] Information Commissioner's Office (ICO), Royal Free - Google DeepMind trial failed to comply with data protection law, 3 July 2017.
[32] Financial Times, Alphabet AI unit urged to clarify its business model.

increases. These features will increasingly allow users to make phone calls, send messages, conduct searches and control other devices from their wearable, whilst leaving their smartphone at home."[33]

There are two important aspects of competition to consider in the context of the wearables market. First, whilst Google is not a manufacturer of wearable devices, it licences its operating system, Wear OS, in a similar fashion to Android in relation to mobile devices.[34] Google's Wear OS runs on smartwatches from manufacturers including Fossil and Misfit,[35] with some Xiaomi and Huawei wearable devices also running this operating system.[36] However, the proposed acquisition could allow Google to implement its Wear OS in Fitbit's devices and impair consumers' choice of smartwatch OS.[37] The ACCC in its Statement of Issues regarding the proposed acquisition raised the concern that Google may foreclose its rivals in the wearables market from competing by limiting their access to Google products currently used by wearable manufacturers (Wear OS, Google Maps, Google Play Store, Android OS).[38] Specifically, in relation to the potential for Google to foreclose access to Wear OS, the ACCC understands that for some manufacturers access to the operating system "*is a critical part of their product offering.*"[39] Indeed, if the proposed acquisition is to take place, foreclosure of access to Wear OS may appear a likely consequence as Google seeks to grow its share of the wearables market. Given the increasing importance of the wearables market, PI believes that the ACCC has an important opportunity to act now to shape the wearables market by ensuring that it remains competitive.

Second, in the absence of competitive pressure to maintain privacy standards after the proposed acquisition (as detailed in Section IV below), consumers of Fitbit's services would be adversely affected by the consequent reduction of competitive pressure as to standards of data privacy in the wearables market. If Google takes away Fitbit users' ability to control their data,[40] forces them to provide more personal data (e.g. through the use of "dark patterns",[41] design strategies that aim to make it difficult to make certain choices over others), and/or imposes more intrusive terms as regards data collection, this will reduce competition as to data privacy with negative connotations for consumers. This will particularly be the case if

[33] ACCC, Statement of Issues: Google LLC – proposed acquisition of Fitbit Inc. (18 June 2020), para 8.
[34] Google, Wear OS.
[35] Ibid.
[36] ACCC, Statement of Issues: Google LLC – proposed acquisition of Fitbit Inc. (18 June 2020), paragraphs 58-59.
[37] Brian Heater, 'Google is acquiring Fitbit for $2.1 billion', TechCrunch, 1 November 2019.
[38] ACCC, Statement of Issues: Google LLC – proposed acquisition of Fitbit Inc. (18 June 2020), para 122.
[39] Ibid, para 126.
[40] See also CMA Market study into online platforms and digital advertising, Interim report (December 2019): Appendix F: Consumer control over data collection.
[41] See, for example, Norwegian Consumer Council "Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy" (27 June 2018).

Google were to impose its Wear OS on future Fitbit devices and seek to foreclose non-Wear OS utilising wearables from the market. As to this, the ACCC provides a clear indication of Wear OS, its role in data collection and the consequences for assessing competition on both the market for wearables, and the markets in which Google is already active.

> "[…] *In addition, the ACCC understands that Google also gains access to the data that is collected by devices running Wear OS. The collection of this data is of potential benefit to Google, and the ACCC will need to weigh this potential benefit when considering Google's incentives to foreclose access to Wear OS.*"[42]

IV. The harmful effects of the acquisition cannot be addressed by accepting remedies

It would not be feasible for the competition concerns caused by the proposed acquisition to be addressed by way of commitments on Google's part.

Google has a long track record of competition law infringements in the EU, including violations of competition on the search market,[43] on Google Play Store and Android[44] and on the market for online advertising intermediation.[45] As the ACCC is well aware, Google is also currently under investigation for other suspected anti-competitive practices in the EU, as well as in the United States[46] and by the ACCC[47], for its conduct in relation to location data. On the data privacy front, Google has also recently been fined EUR 50 million by the French data protection authority (CNIL) for "*failing to provide users with transparent and understandable information on its data use policies*",[48] a decision that was upheld on 19 June 2020 by the French Council of State which dismissed the appeal brought by Google.[49]

---

[42] ACCC, Statement of Issues: Google LLC – proposed acquisition of Fitbit Inc. (18 June 2020), para 129.
[43] 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).
[44] 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.
[45] 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
[46] FT, Which antitrust investigations should Big Tech worry about?.
[47] ACCC, Google allegedly misled consumers on collection and use of location data, 29 October 2019.
[48] CNIL, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019. 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.
[49] CNIL, The Council of State confirms the sanction imposed on Google LLC, 29 June 2020.

Google also has a record of not honouring its privacy commitments in relation to the companies it acquires; ultimately, such commitments are not binding, as noted in the ACCC's SOI regarding the proposed acquisition.[50] For instance, following Google's acquisition of Nest in 2014, Google reportedly strongly encouraged Nest users to migrate from proprietary Nest accounts to Google Accounts since 2019, employing tactics such as providing new features only to those using a Google Account with their Nest devices and requiring new Nest users to sign up with a Google Account.[51] This was contrary to the statements by Nest's CEO at the time of the acquisition that Nest users' data would be ringfenced and prevented from being mixed with Google's existing data.[52]

Similarly, back in April 2007, when Google acquired DoubleClick for $3.1 billion in cash, Google founder Sergey Brin said privacy would be the company's "*number one priority*" when considering new advertising products.[53] That merger was approved by both the European Commission 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. The FTC held that privacy issues were not relevant to an antitrust review.[54] However, following the review of the Google/DoubleClick merger, in the summer of 2016 it was reported that Google had 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.[55]

Needless to say, should Google make any proposed commitments or statements to the effect that data will not be utilised for certain services or may be 'ring-fenced', these proposals should be seen in the context of Google's past conduct in this area.

Further potential remedies which PI anticipates may be suggested, such as in relation to data sharing (access to data by competitors), anonymisation techniques and/or data silos, must also be studied very carefully. Such remedies must not risk proving ineffective in the long run or seriously impair consumers' fundamental freedoms.

Conclusion

[50] ACCC, Statement of Issues: Google LLC – proposed acquisition of Fitbit Inc. (18 June 2020)
[51] Andrew Gebhart, Google will ask you to migrate your Nest account soon: Here's what you need to know, CNET, 12 August 2019.
[52] Leo Kelion, Google-Nest merger raises privacy issues, BBC, 8 August 2018.
[53] Liat Clark, Google's ad-tracking just got more intrusive. Here's how to opt out, Wired UK, 24 October 2016.
[54] Diane Bartz, Google wins antitrust OK to buy DoubleClick, Reuters, 20 December 2007.
[55] Julia Angwin, Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking, ProPublica, 21 October 2016.

The proposed acquisition would have the effect of substantially lessening competition across a number of markets which are vitally important for the development of the digital economy and for consumers.

In the markets for digital ad tech services, Google already occupies an unassailable position of market power. Google should not be allowed to further augment its power in these markets at the expense of consumers.

The markets for data-dependent health services and wearables are, for clear reason, of considerable interest to Google. In relation to each market, the ACCC has the opportunity to act now to preserve and encourage more competitive conditions by retaining the competitive dynamic between Google and Fitbit, by preventing the raising of barriers to entry in the data-dependent health services market and by actively pre-empting the foreclosure of the wearables market.

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