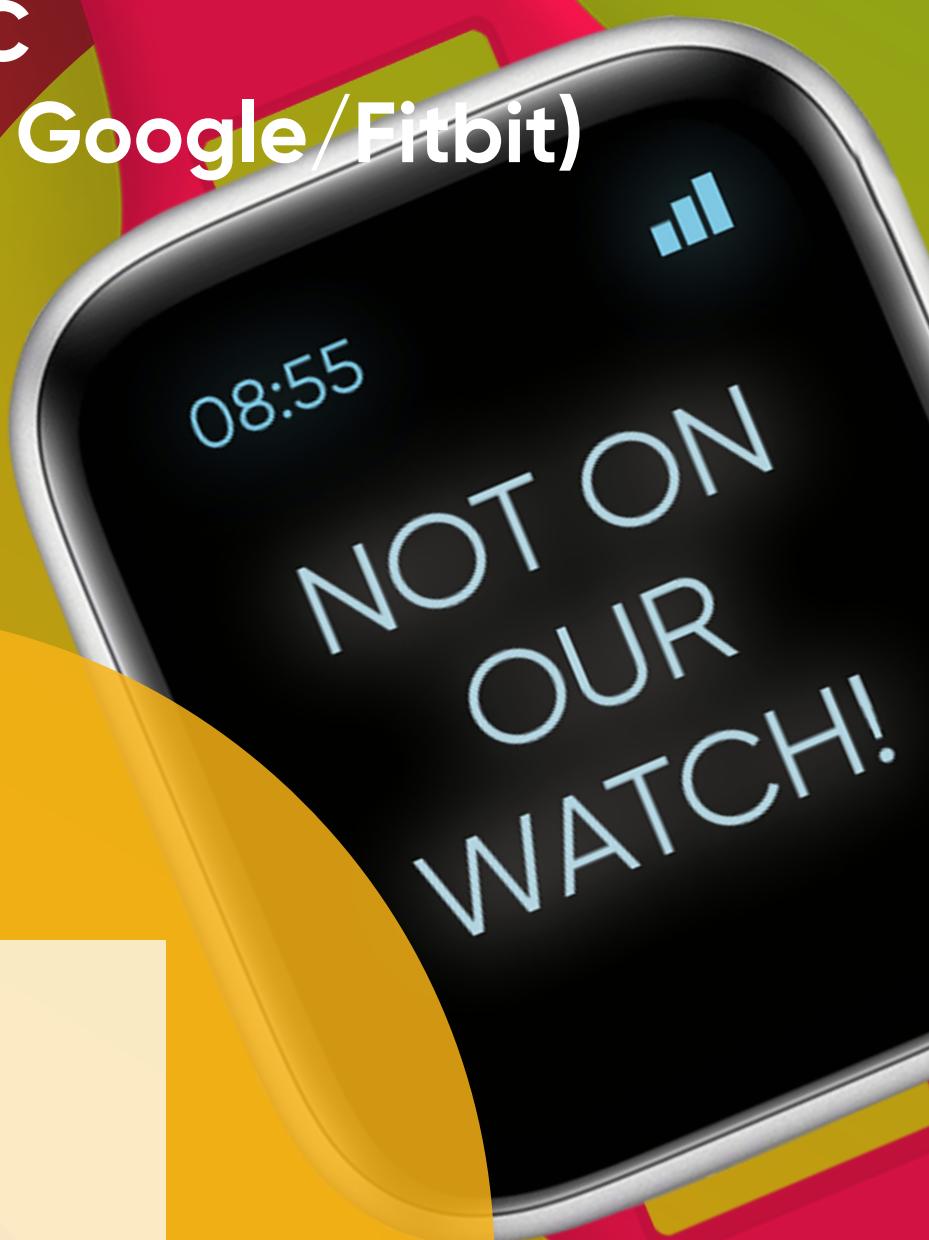
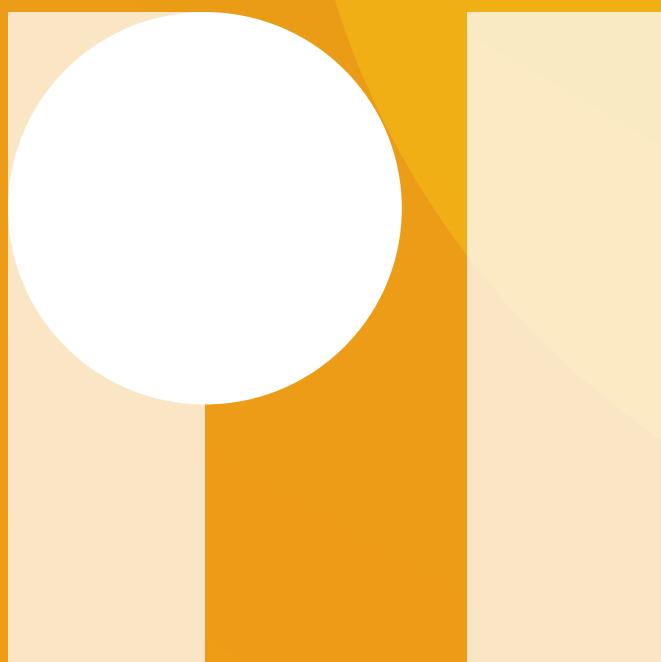


Submission to the European Commission regarding the proposed acquisition of Fitbit, Inc. by Google LLC (Case M.6990 Google/Fitbit)





Submission to the European Commission regarding the proposed acquisition of Fitbit, Inc. by Google LLC (Case M.6990 Google/Fitbit)

Executive summary

This submission comprises Privacy International's ("PI") preliminary comments on Google LLC's ("Google") proposed acquisition of Fitbit, Inc. ("Fitbit") (Case M.6990 Google/Fitbit, the "**proposed acquisition**"), notified to the European Commission (the "**Commission**") for review on 15 June 2020.¹ This submission also constitutes PI's application to be heard as an interested third person as part of the Commission's review.

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 Commission,² the UK Competition and Markets Authority (the "**CMA**")³ and the U.S.

¹ https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=2_M_9660

² 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>.

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>.



Federal Trade Commission ("FTC")⁴ regarding data and competition issues. With regard to the proposed acquisition at issue here, PI has also submitted comments⁵ before the Australian Competition and Consumer Commission (the "ACCC") in the context of its informal review,⁶ and was a signatory to a statement by 20 consumer and citizen groups issued on 2 July 2020 identifying serious concerns with the proposed acquisition.⁷

The proposed acquisition requires very close scrutiny by the Commission. It is highly likely to significantly impede effective competition in several vitally important markets and result in the strengthening of Google's dominant positions, with ramifications for competition and in turn upon consumers and wider society. In particular, the proposed acquisition would:

- further augment Google's dominance in the search and digital advertising markets as Google would benefit from Fitbit's valuable data troves, leading to a further lessening of competition in these markets;
- 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;
- lead to the foreclosure of competitors to Google in the growing wearables market and therefore lead to a lessening of competition in the wearables market; and
- reduce what little pressure there currently is on Google to compete in relation to privacy options available to consumers (both existing and future Fitbit users), leading to even less

⁴ 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>.

⁵ <https://privacyinternational.org/advocacy/3704/submission-australian-competition-and-consumer-commission-proposed-googlefitbit>

⁶ <https://www.accc.gov.au/public-registers/mergers-registers/public-informal-merger-reviews/google-llc-proposed-acquisition-of-fitbit-inc>

⁷ http://www.beuc.eu/publications/beuc-x-2020-060_joint_ngo_statement_on_google_fitbit_merger.pdf



competition on privacy standards and thereby enabling the further degradation of consumers' privacy protections.⁸

The remainder of the submission details PI's interest in the proposed acquisition and sets out PI's initial analysis of the resulting concentration.

(A) Privacy International's interest in the proposed acquisition

PI applies to be recognised as a legal person with sufficient interest in the transaction within the meaning of Article 18(4) of Regulation (EC) No 139/2004 (the "**EU Merger Regulation**")⁹ and Article 11(c) of Regulation (EC) No 802/2004, affording it a right to be heard. PI has a "sufficient interest" in the proposed acquisition within the meaning of these provisions.

PI's application to the Commission is made in its capacity as an organisation seeking to promote consumers' rights and to defend their privacy. Whilst consumers may more usually be perceived as those paying a monetary fee to purchase a good or service, in today's digital markets, we are all consumers of digital technology (including, often, Google's technology) even though we may not pay a fee for these goods and services. Rather we pay with our data, which is conceptualised by some

⁸ 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. In its 2014 assessment of the proposed merger of Facebook and WhatsApp, the Commission acknowledged that "*competition on privacy*" exists. The Commission 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*". In addition, we note that the [CMA's Online Platforms and Digital Advertising Market Study Final Report](#), published on 1 July 2020 (the "**CMA Final Report**"), explicitly refers to privacy as a parameter of competition, see (for example) paragraph 3.12 in relation to search and paragraph 3.158 in relation to social media.

⁹ Article 18(4) states that: "*In so far as the Commission or the competent authorities of the Member States deem it necessary, they may also hear other natural or legal persons. Natural or legal persons showing a sufficient interest and especially members of the administrative or management bodies of the undertakings concerned or the recognised representatives of their employees shall be entitled, upon application, to be heard.*"



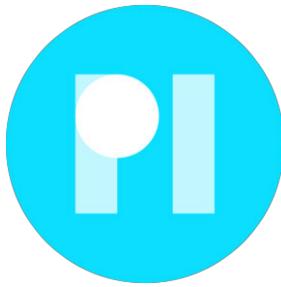
(wrongly, in our opinion) as meaning the good or service is 'free'. That data is then, as the size and value of the digital advertising market makes clear, extremely valuable to the service provider in the upstream market.

The upshot of these transactions on two (or more) sided markets means that the "price" consumers pay for digital services, such as Google's, needs to be understood in the context of the economic value of data¹⁰, and, in turn, that the concept of a "consumer" in this context extends beyond those 'paying' for a service to everyone consuming Google's services. It is the interests of these consumers that PI seeks to represent in the Commission's review of the proposed acquisition.

In particular, the proposed acquisition at its heart concerns a product used by final consumers and an associated trove of data belonging to those consumers, whose interests PI, a legal person, strives to protect. Indeed, the level of interest shown globally in the proposed transaction - and specifically the concerns that have been highlighted relating to the merged entity's use of that data and degradation of consumers' privacy options (a parameter of non-price competition) post-acquisition - indicate that PI is uniquely placed to engage with the Commission on these critical aspects.

As noted above, PI has significant experience and expertise regarding competition issues and interacting with competition regulators, including the European Commission. Most recently, PI made a submission to the ACCC with regard to their investigation of the proposed acquisition. PI also has significant subject-matter expertise: in recent years, PI has conducted extensive research into online

¹⁰ The Commission has acknowledged that tech giants, including Google, value and monetise data in this way, see e.g. case AT.39740 *Google Shopping* at recital 158: "[...] even though users do not pay a monetary consideration for the use of general search services, they contribute to the monetisation of the service by providing data with each query. In most cases, a user entering a query enters into a contractual relationship with the operator of the general search service. For instance, Google's Terms of Service provide: "By using our Services, you agree that Google can use such data in accordance with our privacy policies". In accordance with its privacy policies, Google can store and re-use data relative to user queries. The terms and conditions of other providers of general search services contain similar provisions. The data which users agree to allow a general search engine to store and re-use is of value to the provider of the general search service as it is used to improve the relevance of the search service and to show more relevant advertising." (Footnotes omitted)



platforms and the ad tech industry, exposing¹¹ and filing complaints against¹² several companies' activities insofar as they concern data and competition abuses.

It is without question that the proposed acquisition will impact consumers. In this submission we set out the reasons why the proposed acquisition would also have negative implications for consumers on grounds spanning competition and data privacy, and provide examples of how PI can be of assistance to the Commission in the merger review process through its expertise and the evidence it will adduce concerning data and competition issues.

(B) Privacy International's initial analysis of the proposed acquisition

The remainder of this submission addresses three topics:

- i. First, the importance of examining Google's wealth of consumer data pre- and post-transaction, as an integral part of the Commission's assessment of the competitive effects of the proposed acquisition;
- ii. Second, the impact the proposed acquisition would have on Google's position in the markets for:
 - a. search and search advertising;
 - b. digital advertising and ad tech services;
 - c. digital/data-dependent health services; and
 - d. wearables; and
- iii. Third, why remedies cannot address the competition concerns that arise in the particular circumstances of the proposed acquisition.

¹¹ 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>.

¹² See PI, Challenge to Hidden Data Ecosystem, <https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem>.



(i) The Commission must examine Google's access to and use of consumer data as part of the competitive assessment of the proposed 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 users of their many consumer-facing services, which include the Android operating system, Google Search, YouTube, Gmail, and many others.¹³

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.¹⁴ 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.¹⁵

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 Commission'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

¹³ 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),
<https://www.sec.gov/ix?doc=/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm>

¹⁴ Maurice Stucke and Allen Grunes, *Big Data and Competition Policy*, 2016 Oxford University Press.

¹⁵ In case AT.39740 *Google Shopping* the 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).



asset.¹⁶ Data is also absolutely integral to these companies' business models and therefore their market value.¹⁷ 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.¹⁸

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 the Bundeskartellamt noted in its February 2019 decision against Facebook:

*"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."*¹⁹

¹⁶ 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.

¹⁷ The CMA note in the [CMA Final Report](#) (at paragraph 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.*"

¹⁸ 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.

¹⁹ 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.



The German Federal Court of Justice (Bundesgerichtshof) upheld the Bundeskartellamt's findings in its judgment of 23 June 2020, contradicting the Düsseldorf Higher Regional Court's prior ruling. In its assessment of abuse, the Bundesgerichtshof found that Facebook abuses its dominant position by withholding options for users to limit the use of their data for personalisation of both Facebook content and advertisements on third-party websites that use Facebook's digital advertising tools. As such, privacy is explicitly recognised as a parameter of competition; effective competition in the social media network market would result in privacy safeguards for users, and it is within the remit of a competition authority to act in response to the anticompetitive and privacy-infringing conduct.²⁰

We note that following the announcement of Google's intention to acquire Fitbit, the European Data Protection Board (the "**EDPB**"), in its 18th Plenary Session, adopted a statement underlining 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*".²¹ While PI acknowledges that compliance with data protection laws is fundamentally a matter for data protection regulators, the implications for competition that Google's accumulation of Fitbit's sensitive personal data would have is categorically a matter for the Commission's merger control review, when conducting its ex-ante assessment of the proposed transaction.

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 Commission consider the impact on competition for data privacy when considering the proposed acquisition. Were it to do so, in PI's view, the Commission would conclude that the concentration will cause a significant impediment to effective competition.

²⁰ Bundesgerichtshof, Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook, 23 June 2020

<https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html?nn=10690868>.

²¹ https://edpb.europa.eu/news/news/2020/eighteenth-edpb-plenary-session_en



PI is liaising with [REDACTED]
[REDACTED], for the purposes of providing more information to the Commission on the value of data in the digital economy.

(ii) The impact of the proposed acquisition on consumers of Google's services

The proposed transaction would significantly impede effective competition in three sectors in particular: (a) the search and search advertising markets, where Google's already dominant positions would be further entrenched; (b) the markets for digital advertising and ad tech services, where again Google's already dominant positions would be further reinforced by the additional sensitive personal data it would acquire from Fitbit; and (c) the digital or data-dependent health services market, in which actual/potential competitors would struggle to compete with a combined Google/Fitbit and its unrivalled quantity and quality of sensitive personal health-related data.

a. Search and search advertising markets

The proposed acquisition would reinforce Google's market power in the search and search advertising markets, in which Google already holds a very significant dominant position. With regard to search, the Commission in its *Google Shopping*²² and *Google Android*²³ Decisions found Google to hold a dominant position in national markets of EU Member States for general search services. Similarly, the CMA Final Report recently found that "*Google has generated around 90% or more of UK search traffic each year over the last ten years and generated over 90% of UK search advertising revenues in 2019.*"²⁴

Google leverages its dominance in search into the market for search advertising, where it also holds an overwhelmingly dominant position. With regard to search advertising, the Commission's press

²² Case AT.39740 *Google Shopping* at Section 6.2

https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf

²³ Case AT.40099 *Google Android* at Section 11.3.4.2

https://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf

²⁴ [CMA Final Report](#), paragraph 18



release announcing its *Google AdSense* Decision noted that "[i]n 2016 Google ... held market shares ... above 75% in most of the national markets for online search advertising" and also found Google to be dominant in the online search advertising intermediation market.²⁵ The CMA Final Report also notes that "Google has continued to account for more than 90% of search advertising revenues"²⁶ and underlines the role data plays in allowing Google to maintain its strong position in these markets:

"Google's extensive first-party data²⁷ is likely to give it a substantial advantage over smaller rivals, creating a barrier to entry and expansion. As a result of Google's first-party data, advertisers on Google can target search advertising to particular audiences (and have confidence in the composition of those audiences), allowing improved performance for their advertising. Google also has access to extensive data on user location, including through Android phones, on which half to two thirds of users have location services activated; this allows search advertising to be more effectively targeted based on location.

Google's data further allows it to offer more accurate attribution services to advertisers. Google has tags (including as a third-party) on over 80% of websites and over 85% of apps on the Play Store, which allows it to form a more complete picture of users' ad exposures, across its own properties and a substantial proportion of other non-Google websites. This allows Google to attribute conversions more accurately to the multiple ad exposures. Its location data also creates the potential to monitor some offline as well as online activity – for example by tracking whether someone is in a particular store.

Several advertisers highlighted Google's first-party data as an advantage over Bing.²⁸

²⁵ https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770

²⁶ [CMA Final Report](#), paragraph 5.46.

²⁷ First-party data is defined as "First-party data is information that a business collects directly from its users rather than via a third party."

²⁸ [CMA Final Report](#), paragraphs 5.60-5.62.



Fitbit's technologies collect and process vast quantities of health-related data, including tracking distance walked or travelled, calories burned, sleep patterns, heart rate, menstruation cycles and likely fertility windows (the "**Fitbit data**").²⁹ The quality as well as the quantity of this data is highly valuable: indeed, the Fitbit data is a large part of Fitbit's value to Google.³⁰ If Google is permitted to acquire Fitbit's data, Google's unrivalled market power in search and digital advertising will only grow, further entrenching its already super-dominant position in both markets.

We note in particular that the proposed acquisition would grant Google unprecedented access to sensitive data. PI has analysed Fitbit's privacy policy and data collection practices through its own research on one of Fitbit's fitness trackers and the Fitbit mobile phone app and the results of this analysis are annexed to this submission. PI is liaising with [REDACTED] [REDACTED], for the purposes of providing more information to the Commission on the potential value of Fitbit's data to Google.

b. Digital advertising/ad tech services

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.

The degree of Google's existing market power in digital advertising is not without consequence for consumers. We note that the CMA Final Report identifies various competition concerns which are

²⁹ Fitbit, Fitbit Privacy Policy, Effective 18 December 2019, <https://www.fitbit.com/au/legal/privacy-policy#info-we-collect>.

³⁰ 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>.



only likely to increase in significance should the proposed acquisition be permitted. In particular, the CMA found that where competition is not functioning well, consumers are impacted by a lesser degree of innovation and higher costs from digital advertising passed on to consumers in the form of inflated prices for goods and services. Importantly, consumers are also inadequately compensated for their data and attention and less able to exercise control over their data.³¹ The CMA notes also that access to data is an important parameter of competition in digital advertising, as data enables both personalised advertising and measuring outcomes. Against this background, it is unquestionable that access to data from Fitbit devices will be of considerable value to Google in the digital advertising market.

This reduction in competition will undoubtedly affect consumers. As we refer to above, competition in digital markets takes place along various price and non-price parameters, with examples of the latter being quality, innovation and privacy. The importance of non-price parameters is to be expected, as the ‘price’ for service usage which consumers must pay is more often than not that of their data.

However, in data-intensive digital markets characterised by increased corporate concentration, as those of search and digital advertising are, Google, as the occupant of dominant positions, has very little incentive to adopt a business model and/or practices which enhance consumers' privacy. Google's acquisition of Fitbit would further reduce any competitive pressure on Google to compete on these non-price (i.e. quality, privacy) aspects, since the acquisition would further entrench Google's dominance and preclude the possibility of competition from another entity acquiring/partnering with Fitbit to compete with Google in this space.

c. 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

³¹ [CMA Final Report](#), paragraphs 6-13



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 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 can be used alongside the services.³² The joint venture was cleared unconditionally in February 2016.³³
- In October 2018, the 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.³⁴
- Last year it was revealed that Google has partnered with Ascension, the second largest healthcare provider in the US.³⁵ As part of the so-called "Project Nightingale", Google has

³² 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, 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.

³³ In its [clearance decision](#) (Case M.7813 - Sanofi/Google/DMI JV, 23 February 2016), the 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).

³⁴ Case M.8991 – Alphabet/ResMed/JV

³⁵ <https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790>



supposedly received healthcare information of up to 50 million Americans, including sensitive information such as names and medical history, without anonymisation.³⁶

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 Commission 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:

- In 2015, 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 2012.³⁷ 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.³⁸

³⁶ <https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information>

³⁷ 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>.

³⁸ 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>.



- 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.³⁹

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.

d. Wearables

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 note in their Statement of Issues:

"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 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." ⁴⁰

³⁹ Financial Times, Alphabet AI unit urged to clarify its business model, <https://www.ft.com/content/215062da-6fe3-11e8-852d-d8b934ff5ffa>.

⁴⁰ ACCC, Statement of Issues – Google LLC – Proposed acquisition of Fitbit Inc, 18 June 2020, <https://www.accc.gov.au/system/files/public-registers/documents/Google%20Fitbit%20-%20Statement%20of%20Issues%20-%2018%20June%202020.pdf>.



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.⁴¹ Google's Wear OS runs on smartwatches from manufacturers including Fossil and Misfit,⁴² with some Xiaomi and Huawei wearable devices also running this operating system.⁴³ However, the proposed acquisition could allow Google to implement its Wear OS in Fitbit's devices and impair consumers' choice of smartwatch OS.⁴⁴ 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).⁴⁵ 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.*"⁴⁶ 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 Commission 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 we set out above in the context of the search, digital advertising markets and data-dependent health markets), 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

⁴¹ <https://developer.android.com/wear>

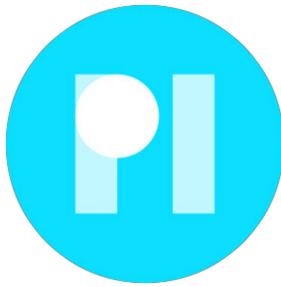
⁴² Ibid

⁴³ ACCC, Statement of Issues – Google LLC – Proposed acquisition of Fitbit Inc, 18 June 2020, paragraphs 58-59
<https://www.accc.gov.au/system/files/public-registers/documents/Google%20Fitbit%20-%20Statement%20of%20Issues%20-%202018%20June%202020.pdf>

⁴⁴ <https://techcrunch.com/2019/11/01/google-is-acquiring-fitbit/>

⁴⁵ ACCC, Statement of Issues – Google LLC – Proposed acquisition of Fitbit Inc, 18 June 2020, paragraph 122
<https://www.accc.gov.au/system/files/public-registers/documents/Google%20Fitbit%20-%20Statement%20of%20Issues%20-%202018%20June%202020.pdf>.

⁴⁶ ibid, paragraph 126



market. If Google takes away Fitbit users' ability to control their data,⁴⁷ forces them to provide more personal data (e.g. through the use of "dark patterns",⁴⁸ 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 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."*⁴⁹

(iii) 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.

⁴⁷ See also CMA, Interim report (December 2019): Appendix F: Consumer control over data collection.

⁴⁸ 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), <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

⁴⁹ ACCC, Statement of Issues – Google LLC – Proposed acquisition of Fitbit Inc, 18 June 2020, paragraph 129 <https://www.accc.gov.au/system/files/public-registers/documents/Google%20Fitbit%20-%20Statement%20of%20Issues%20-%2018%20June%202020.pdf>.



Google has a long track record of competition law infringements in the EU, including violations of competition on the search market,⁵⁰ on Google Play Store and Android⁵¹ and on the market for online advertising intermediation.⁵² As the Commission is well aware, Google is also currently under investigation for other suspected anti-competitive practices in the EU, as well as in the United States⁵³ and by the ACCC⁵⁴, for its conduct in relation to location data. And 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”,⁵⁵ a decision that was upheld on 19 June 2020 by the French Council of State which dismissed the appeal brought by Google.⁵⁶

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 Statement of Issues

⁵⁰ 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\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1516198535804&uri=CELEX:52018XC0112(01)).

⁵¹ 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.

⁵² 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.

⁵³ FT, Which antitrust investigations should Big Tech worry about?, <https://www.ft.com/content/abcc5070-f68f-11e9-a79c-bc9acae3b654>.

⁵⁴ 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>.

⁵⁵ 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>. 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.

⁵⁶ <https://www.cnil.fr/en/council-state-confirms-sanction-imposed-google-llc>



regarding the proposed acquisition.⁵⁷ For instance, following Google's acquisition of Nest in 2014, Google has been reported to strongly encourage 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.⁵⁸ 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.⁵⁹

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.⁶⁰ 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.⁶¹ 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.⁶²

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.

⁵⁷ ACCC, Statement of Issues – Google LLC – proposed acquisition of Fitbit Inc, 18 June 2020, <https://www.accc.gov.au/system/files/public-registers/documents/Google%20Fitbit%20-%20Statement%20of%20Issues%20-%2018%20June%202020.pdf>

⁵⁸ <https://www.cnet.com/how-to/google-will-ask-you-to-migrate-your-nest-account-soon-heres-what-you-need-to-know/>

⁵⁹ <https://www.bbc.com/news/technology-42989073>

⁶⁰ <https://www.wired.co.uk/article/google-ad-tracking>

⁶¹ <https://www.reuters.com/article/us-doubleclick-google/google-wins-antitrust-ok-to-buy-doubleclick-idUSN2039512220071220>

⁶² 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>.



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.

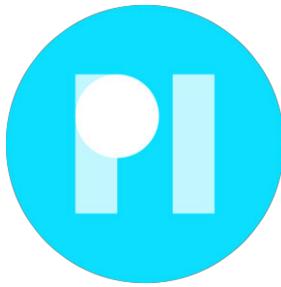
For example, the last two decades have shown that robust anonymisation of personal data is very difficult to achieve effectively, and that measures that may be effective today may not be tomorrow. New techniques are regularly developed which allow re-identification of individuals; this is especially true for high-dimensional and granular data such as that processed by the range of Fitbit products. A primary source of value in Fitbit's data may be the possibility of building machine learning models based on the cardiac rhythms, exercise, location, and sleep cycles of Fitbit users (see Annex I). Even if these models are not explicitly intended to match individuals between datasets, they could potentially be at risk of 'model inversion', where models themselves contain traces of the personal data they were trained on. PI is liaising with [REDACTED] [REDACTED], for the purposes of providing more information to the Commission on this topic.

Conclusion

In light of the considerations outlined in this submission, PI considers that the proposed acquisition would have the effect of significantly impeding effective competition across a number of markets which are vitally important for the development of the digital economy and for consumers.

In the markets for search and search advertising, as well as 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.

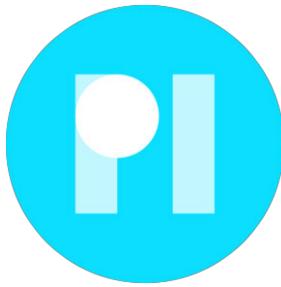
The markets for data-dependent health services and wearables are, for clear reason, of considerable interest to Google. In relation to each market, the Commission has the opportunity to act now to preserve and to encourage more competitive conditions by retaining the competitive dynamic



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.

PI therefore respectfully suggests that the Commission ought to apply a high level of scrutiny to the acquisition, including thoroughly assessing the impact such further concentration of data would have on the competitive landscape post-acquisition.

Further and as set out above, PI wishes to participate in the Commission's review of the proposed acquisition as an interested third person representing the interests of consumers whose data privacy rights would be adversely impacted by the proposed acquisition, in particular as a result of reduced incentives to compete on non-price parameters (especially privacy protections) post-acquisition. We would be pleased to engage further with the Commission on any aspect of this submission, including providing further information on any of the issues referred to above.



ANNEX ONE

1. Introduction

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.⁶³ In 2019 Fitbit reported a revenue of \$ 1,435 billion.⁶⁴

A big part of Fitbit's value is said to lie in the quality of the health data it possesses.⁶⁵ The company's technologies can track individuals' daily steps, distance walked or travelled, calories burned, sleep patterns and heart rate.⁶⁶ In 2018, Fitbit also introduced 'female health tracking' to track menstruation cycles and likely fertility windows.⁶⁷ In the recent past, Fitbit has further increased its health-related database and health tracking capabilities by acquiring a number of other actors in the health tracking and wearables market, including FitStar, Pebble, Vector and Twine Health. Some of these acquisitions include partnerships with health insurers,⁶⁸ as part of efforts to diversify its revenue stream.⁶⁹

The analysis below seeks to demonstrate the extent of Fitbit's data collection practices, which often involve the processing of sensitive special-category personal data. Should Fitbit's acquisition by Google be approved, 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,

⁶³ <https://www.fitbit.com>.

⁶⁴ 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>.

⁶⁵ 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>.

⁶⁶ Fitbit, Fitbit Privacy Policy, Effective 18 December 2019, <https://www.fitbit.com/au/legal/privacy-policy#info-we-collect>.

⁶⁷ 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>.

⁶⁸ 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>.

⁶⁹ 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>.



general search, wearables and health care/health services markets. The terms Fitbit and Fitbit services are used interchangeably throughout this Annex and they should be deemed to mean Fitbit, Inc. as well as its devices, applications, software, websites, APIs, products, and services.

This analysis is predominantly based on Fitbit's Privacy Policy (effective: 18 December 2019), which is attached to this Annex and can also be found here:

<https://www.fitbit.com/uk/legal/privacy-policy#analytics-and-advertising>. 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 Privacy International ("PI") staff, which involved the occasional use of a Fitbit "Charge 3" device⁷⁰ and its association with PI staff personal smartphone(s), together with a Fitbit premium subscription.⁷¹

2. Categories of personal data obtained by Fitbit

2.1. 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:

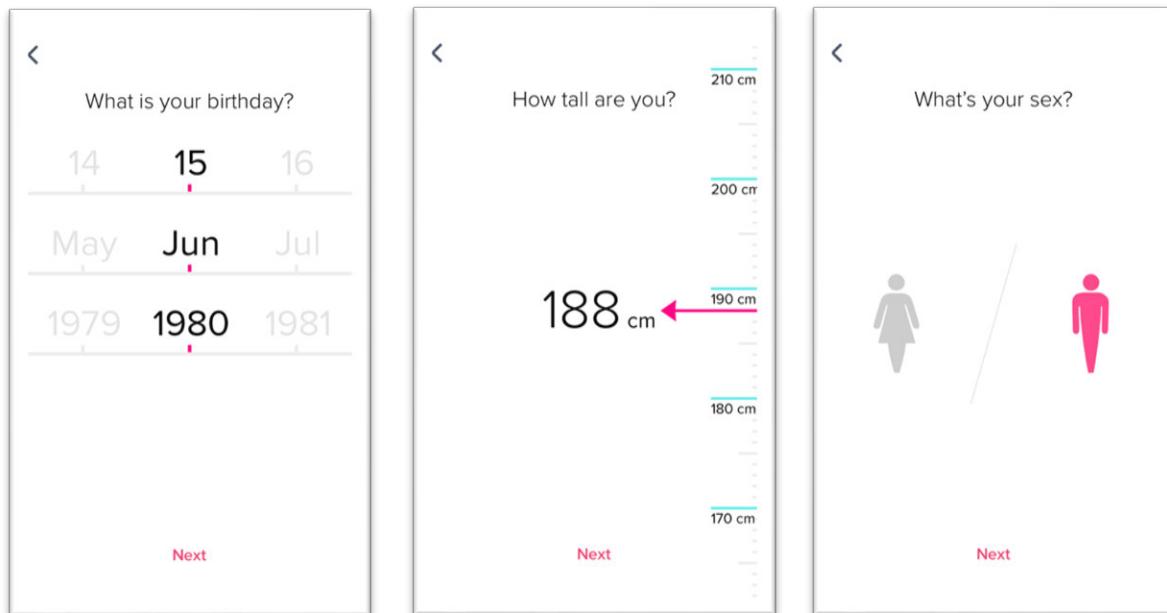
name, email address, password, date of birth, gender, height, weight, and in some cases your mobile telephone number. This is the only information you have to provide to create an account with us. You may also choose to provide other types of information, such as a profile photo, biography, country information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

⁷⁰ Fitbit Charge 3 product page on Fitbit's website: <https://www.fitbit.com/uk/charge3>.

⁷¹ <https://www.fitbit.com/uk/fitbit-premium>.



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



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 or special-category personal data not only in relation to health data but also with regard to other sensitive, special-category 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.

Female Health

Are you using a birth control method?

Because some types of birth control may alter your period or fertile window, having this info could help improve your predictions and insights in the future.

Yes, I'm using birth control

No

Injection/shot

Vaginal ring

Implant

Patch

Condom (feminine/masculine)

Non-hormonal IUD

Sterilization

Next

Back Calendar Trends

M T W T F S S

TODAY 21 22 23

17 18 19 20 21 22 23

24 25 26 27 28 29 1

2 3 4 5 6 7 8

9 10 11 12 13 14 15

16 17 18 19 20 21 22

7 Mar 2020

Ovulation Day

Cycle day 15 of 28

Log Details

How to add and edit periods

Touch and hold a calendar day to enter edit mode! Easy peasy. [Learn more](#)

Got it!

Cancel Log Details Save

FLOW INTENSITY

17 18 19 20 21 TODAY 22 23

Logging flow intensity will not add a period day. To add or edit a period, enter the edit mode from the calendar by touching and holding a day or tapping the pencil icon.

SPOTTING Light Medium Heavy

SYMPTOMS

Cramps Headache Bloated Acne Hot Flashes

MOOD

Happy Sad Energized Fatigued Anxious Str

SEX

Protected Unprotected

OVULATION TEST

Positive Negative

FLUIDS

Egg White Creamy Sticky Unusual

OTHER EVENTS

Morning After Pill

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 Coach⁷², 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.

2.2. 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,

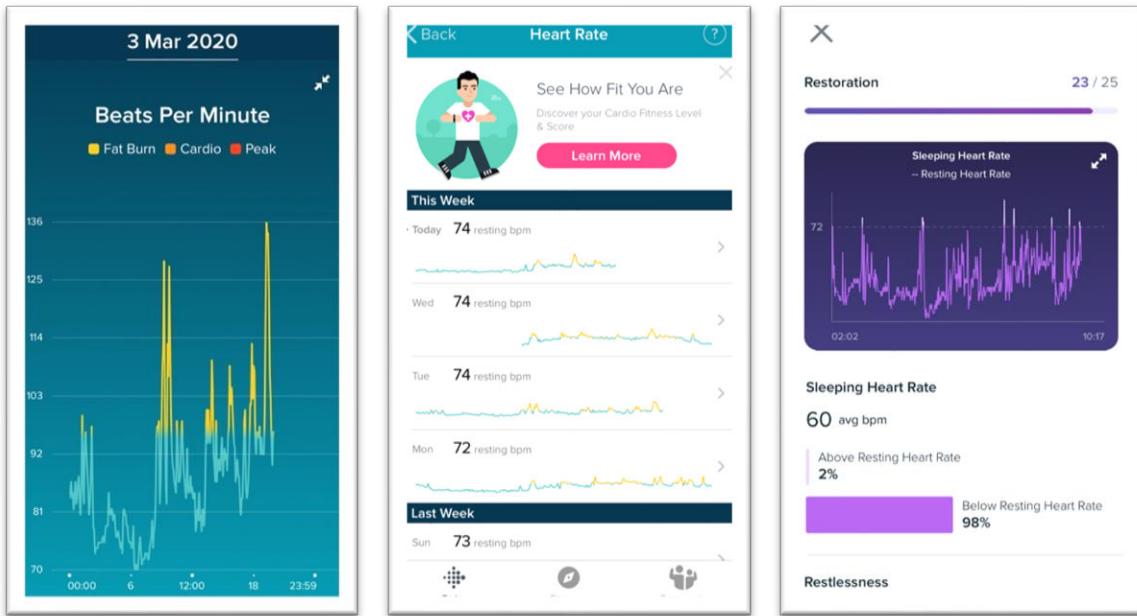
⁷² <https://coach.fitbit.com>



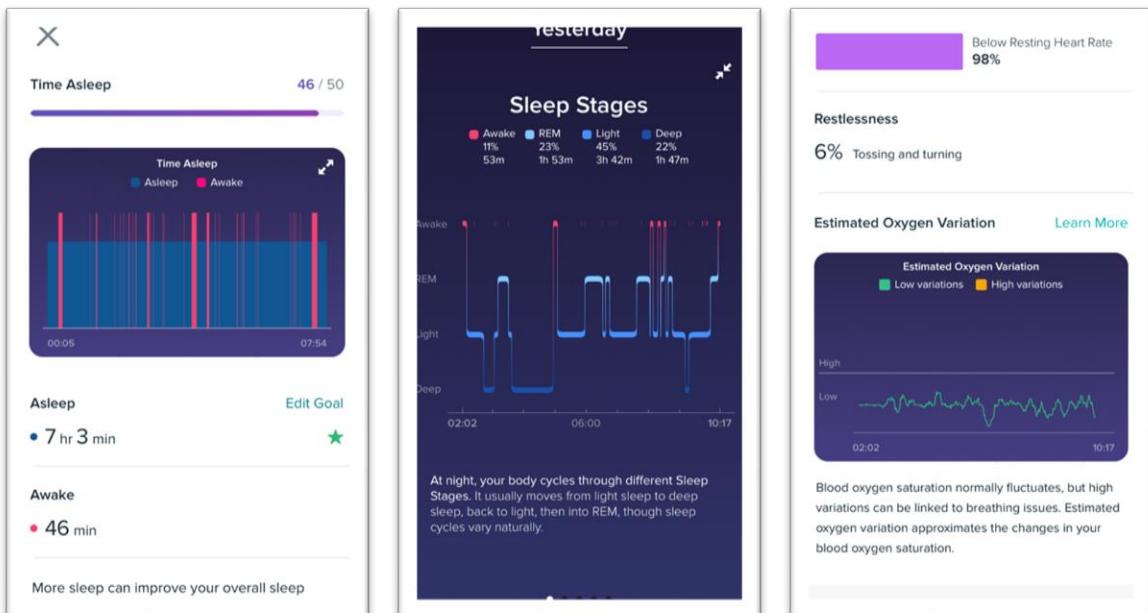
the table below provides an overview of the categories of personal data collected within the ambit of these three wider categories.

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.

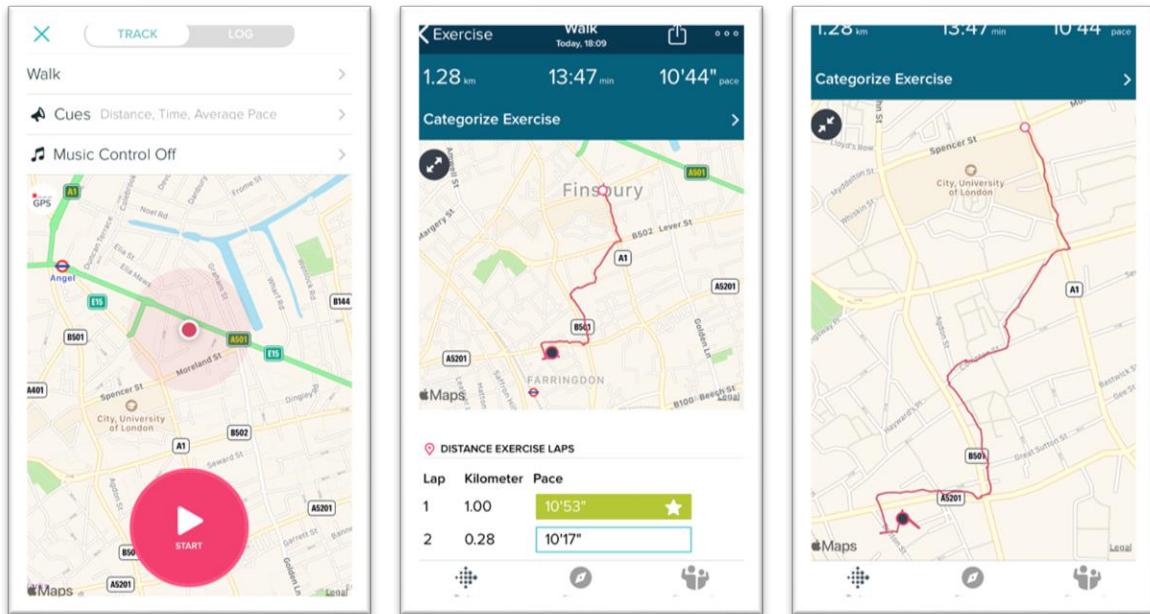
The screenshots below seek to complement some of the categories of personal data mentioned in the table above, highlighting the extent of Fitbit's data collection and the sensitive nature of the personal data that Fitbit service might obtain.



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.



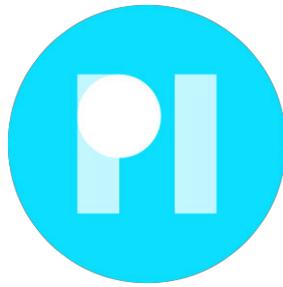
Geolocation data: Examples of GPS tracking data collected by Fitbit.

2.3. 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.

2.4. 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.

3. Conclusion

This analysis has highlighted the extent of personal data collection of the Fitbit services. As it is shown above, Fitbit's data collection practices do not only cover large amounts of various categories of personal data but may also likely involve extremely sensitive, special-category data, such as data relating to health or data concerning a natural person's sex life or sexual orientation.⁷³ Several of

⁷³ 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



these categories of personal data, such as geolocation, sleep pattern inferences and other profiling etc, may not be collected directly from users but from their devices or usage or network activity instead. 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.

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.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org