PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

7 January 2020

Fitbit
Sent via: https://help.fitbit.com
and via Twitter @fitbit

Dear Sir/Madam,

RE: Cloud analytics: Request for response regarding potential misuse of your customer data

It is apparent from our research (attached and here) that your products can be accessed using Oxygen Forensics Cloud Extractor and Cellebrite UFED.

We therefore **seek a response from you on your position on the use of cloud analytics technologies by law enforcement** to obtain cloud stored data as we believe the use of these technologies presents a significant issue for the security of your customers' data.

Oxygen Forensics states that:

> "Many of today's users are into health wearables, from the Fitbit to the Apple Watch, which includes information such as heart rate, location, food intake, messaging and other valuable data that is often available only on the cloud service and not on the mobile device."

Cellebrite states that it can access Fitbit "user profile, logs, activities, goals, friends, heart rate, exercise track (speed, location, time etc)."

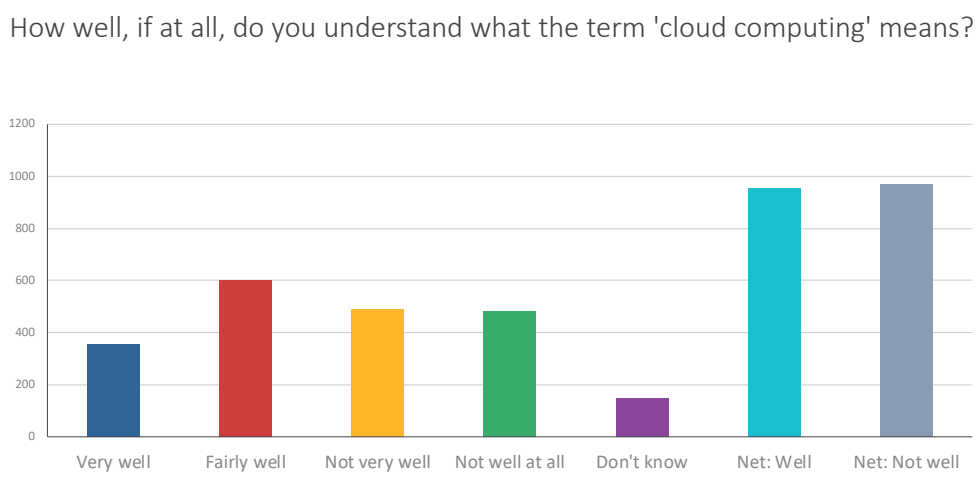
Please respond no later than **17 January 2020**. Please note that we will assume we can publish your response unless you state otherwise. If we do not hear from you, we will publish that you have not responded.

Summary of the research

- Law enforcement are increasingly using cloud analytics[1]
- This can be used to obtain vast quantities of your customers' data outside the normal legal frameworks for obtaining customer data in the course of criminal investigations e.g. via warrant to Fitbit.
- Emotion and facial recognition can be applied to your customers' data
- Cloud analytics software is being used without any transparency and in the absence of clear, accessible and effective legal frameworks
- There is a risk of abuse and misuse of customer data and miscarriage of justice

Your customers need you to protect their data

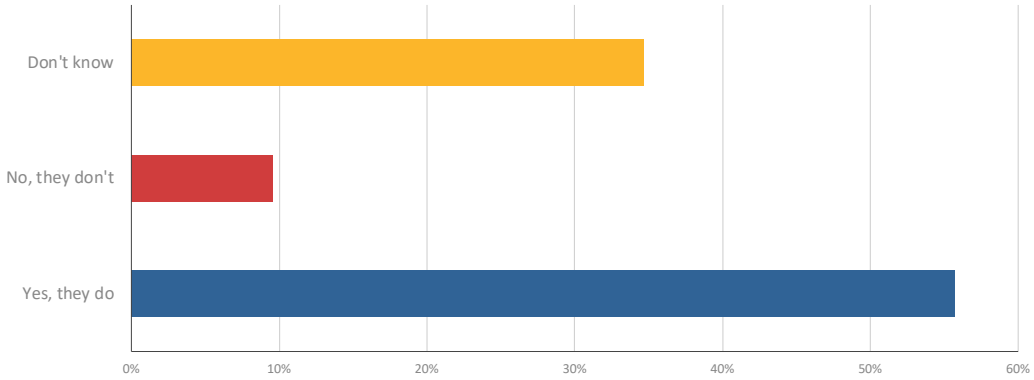
Our research has shown that your customer data can be accessed using cloud extraction software and hardware. Despite the fact that you store your customer data in the Cloud, a YouGov poll[i] revealed that a large number of individuals in the UK who do not understand the term 'cloud computing'.



The results also showed that 45.6% of people have not thought about where data created by apps on their phone is stored and 44.3% of people do not know or think that apps on their phone use cloud storage.

[1] Cellebrite, a prominent vendor of surveillance technology used to extract data from mobile phones, notes in its Annual Trend Survey that in approximately half of all investigations, cloud data 'appears' and that '[t]ypically, this data involves social media or application data that does not reside on the physical device.' That it 'does not resides on the physical device' indicates that law enforcement is turning to 'cloud extraction'.

Do any of the apps on your smartphone use cloud storage?



We believe that it is a serious concern that people don't where their data is stored, but the police do - and they can access vast troves of highly sensitive data at the push of a button.

We look forward to hearing from you.

Kind regards,

Camilla Graham Wood
Privacy International

[i] All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 2072 adults. Fieldwork was undertaken between 7th - 8th November 2019. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18+).