WEARABLES AND FITNESS APPS: DATA COLLECTION UNCHAINED

MARKTWÄCHTER DIGITALE WELT

Smartwatches, tracker bands and fitness apps: the boom in wearables and applications (apps) in the fitness and health sector shows no sign of slowing down. What is more, for some time now, these smart companions do more than to just count steps. They know how long and how well users sleep, monitor their pulse and calorie consumption, and overall know whether they are active or not. All of this represents sensitive personal data which allows for far-reaching conclusions about consumers' fitness and overall health. What happens with the data collected, though, and do users have any control over it?

As part of the "Market Watch Digital World" project, the Consumer Association of North Rhine-Westphalia (Verbraucherzentrale NRW, VZ NRW) has examined twelve wearable devices and 24 fitness apps to find out just what kind of data they register, which servers they transfer it to, and how safe this data transfer is from unauthorised access. VZ NRW has also looked at the providers' approaches to data protection regulations and conducted a representative survey of consumers which shows that privacy is an important concern when it comes to wearables and fitness apps.

Results of the representative survey

CONCERNS ABOUT PRIVACY: CONSUMERS FEAR LOSING CONTROL OF DATA

Among both those who use wearables and those who do not, a majority of consumers are concerned about how data collected about them online is used and do not want to lose control of their personal data. There is a range of opinions about the potential consequences of using wearables. Many consumers say they would not have a problem with the idea of data from the devices being used to cross-check witness statements (61%) or as part of employer bonus programmes (44%). However, only a small minority would be willing to accept an increase in their own health insurance contributions based on fitness data (13%).

Results of the technical examination

DATA COLLECTION UNCHAINED

Technical examinations of twelve wearables and 24 fitness apps showed that it is almost impossible for users to retain control of their data. Most of the apps send a multitude of personal, often sensitive data to the providers' servers, including third parties such as analytics or advertising services. 16 of the 19 apps which work with third parties send technical details (e.g. device operating system) before consumers could even accept the terms of use or had the possibility to be notified of how their data will be used. One positive result was that all of the apps examined transferred all user data using https-encoding. Nevertheless, only few of the tested wearables[1] offer protection from unwanted location tracking; this makes it possible to produce records of users' exact movements.

Results of the legal evaluation[2]

PROVIDERS KEEP CUSTOMERS IN GREY AREAS ABOUT DATA USE

Although providers have a legal duty to inform customers about how data collected about them will be used, the VZ NRW's Market Watch experts reached the conclusion that, in many of the cases examined, this duty had been neglected. Three of the providers offer their privacy policies in English only, and only two inform users about the special status of health-related data. Only one single provider includes a separate agreement with users about processing this sensitive data. Five of the providers retain the right to pass users' personal data on if they merge with or are taken over by another company. What is more, a textual analysis provides clear grounds to suspect that many consumers will have difficulty reading and understanding the provisions of these privacy policies.

Conclusion of the investigation

CONSUMERS' CONCERNS ARE LEGITIMATE

The results of the technical examination and legal evaluation of wearables and apps shows that consumers' concerns are by no means unfounded: a lack of protection from unwanted tracking, a high rate of data transfer, and a lack of opportunities for users to check on data use show that improvements are needed in data protection and security.

verbraucherzentrale

[1] During inactive pairing, i.e. when the connection between wearable and smartphone is interrupted.

[2] Data protection statements were last accessed on 5th September 2016; any provider updates to their privacy policies since that date do not form part of the evaluation.

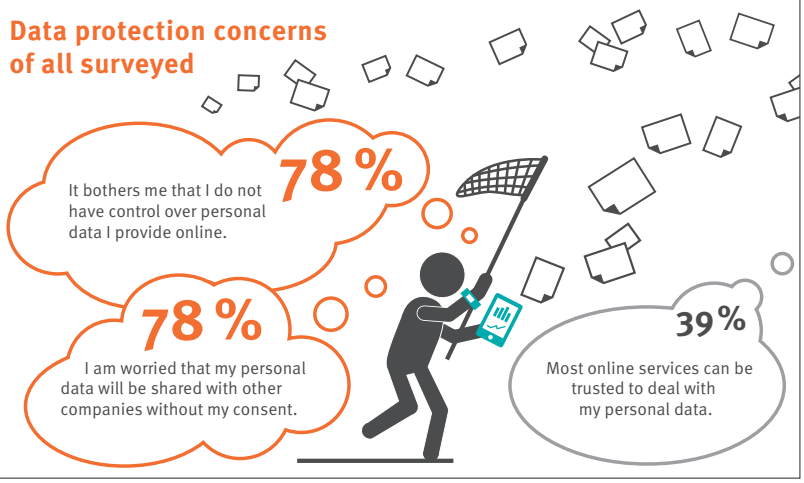
WEARABLES AND FITNESS APPS

DATA PROTECTION CONCERNS: CONSUMERS FEAR LOSING CONTROL

MARKTWÄCHTER DIGITALE WELT

What are consumer concerns about wearables, fitness apps, and data protection? And how do they view potential consequences of using services?

Data protection concerns of all surveyed

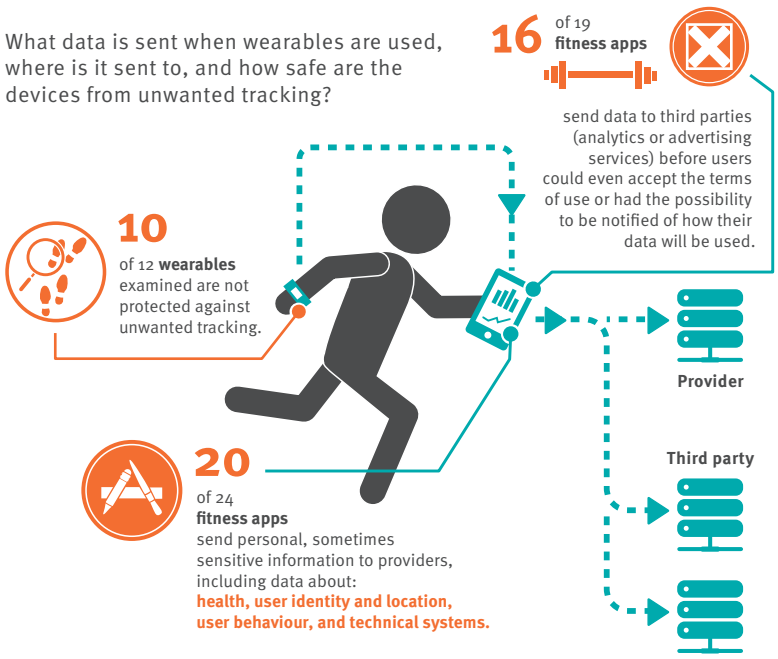


Source: "Wearables, fitness apps, and data protection" – A survey by German Consumer Associations as part of the Market Watch Digital World project.
Method: Results on the basis of a representative telephone survey of 1055 people over 14 years of age who used the internet at some point in the last three months.
Date of survey: 25/08 - 29/09/2016
Survey institute: mindline media GmbH
Margin of error of whole sample: max. +/-3% (at a share of 50%)

DATA COLLECTION UNCHAINED: FITNESS APPS SHARE CONSUMER DATA

MARKTWÄCHTER DIGITALE WELT

What data is sent when wearables are used, where is it sent to, and how safe are the devices from unwanted tracking?



Source: "Wearables, fitness apps, and data protection" – A survey by German Consumer Associations as part of the Market Watch Digital World project.
Method: Examinations were carried out on twelve wearable devices and the matching fitness apps for the iOS and Android operating systems.
Date of survey: 01/07 - 11/08/2016
Survey institute: datenschutz nord GmbH

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

As at: April 2017

verbraucherzentrale

PUBLISHED BY:
Verbraucherzentrale NRW e.V.
Mintropstr. 27
40215 Düsseldorf

The "Wearables, fitness apps, and data protection" investigation was carried out as part of the Market Watch Digital World project.