WEARABLES AND FITNESS APPS:
DATA COLLECTION UNCHAINED

Market Watch experts reveal lack of data protection in new fitness technology

Düsseldorf/Berlin 26th April 2017 – When it comes to data protection, wearables and fitness apps are lacking, as is revealed in an investigation by the Consumer Association of North Rhine-Westphalia (Verbraucherzentrale NRW, VZ NRW). The organisation’s “Market Watch Digital World” team took a close-up look at twelve wearables and 24 fitness apps – and found that the majority of these apps send large amounts of information, including health-related details, to the providers. According to the Market Watch experts, hardly any of the privacy policies of the companies whose products were examined provide consumers with sufficient information about how this data is used. As a result, the VZ NRW’s Market Watch experts have sent cease and desist orders to nine providers regarding a range of breaches of privacy law.

Smartwatches, tracker bands, and fitness apps do more than to just count steps: these smart companions monitor users’ pulses and calorie consumption, or how long and how well they sleep. “This kind of information allows for far-reaching conclusions about consumers’ fitness and overall health,” stresses Ricarda Moll (VZ NRW, Market Watch Digital World), “and that is one reason why we have carried out a detailed investigation into wearables and fitness apps from a consumer’s perspective.” What data do the devices and applications collect? Which servers do they transfer it to? And how safe is this data transfer from unauthorised access? What is more: what approaches do the providers take to data protection regulations? In addition to these technical and legal examinations, the Market Watch team also commissioned a consumer survey to find out what their concerns are about data protection.

CONSUMERS WORRIED ABOUT THEIR DATA

The results of the representative survey show that the majority of respondents were concerned about what happens with data collected about them on the internet. By a large margin, they are unhappy with the lack of control they have of personal data
they provide online (78%), while there is a range of opinions about the potential consequences of using wearables. For example, a relatively high percentage of 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%).

CONTROLLING PERSONAL DATA IN APPS ALMOST IMPOSSIBLE

The results of the technical examinations of twelve wearables and 24 fitness apps showed that it is almost impossible for consumers to retain control of their data. Most of the apps the Market Watch experts looked at send a multitude of personal, often sensitive data to the providers’ servers, and often include 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 of the investigation was that all of the apps examined transferred all user data using a safe connection (https-encoding). Nevertheless, very few of the wearables looked at offer any way of guarding against unwanted location tracking. This makes it possible to produce records of users’ exact movements.

LEGAL LIMBO AROUND DATA USE

As a result of their legal analysis, the Market Watch experts have reached the conclusion that the companies behind the products examined frequently leave consumers in a legal limbo with regards to how data collected about them will be used. For instance, 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 makes a separate agreement with users about processing this sensitive data. Another serious issue is that six companies reserve the right to implement changes to their privacy policy at any time without actively informing users; five of the providers even retain the right to pass users’ personal data on if they merge with or are taken over by another company.

CEASE AND DESIST ORDERS FOR PROVIDERS

Following the investigation, the Market Watch team at the VZ NRW sent cease and desist orders to nine providers regarding a variety of breaches of privacy laws. “Consumers are concerned about data collected about them online – and now we can confirm that their concerns are legitimate,” says Moll. “Providers are collecting a multitude of (sometimes sensitive) data and leaving many consumers in the dark regarding its use. We are not willing to accept this state of affairs.”
CREATING TRANSPARENCY AND UPHOLDING UNIVERSAL HEALTH INSURANCE

“The bewildering array of wearables and fitness apps on the market and a new generation of digital services in development have the potential to collect and transmit sensitive data regarding the health of individual users to providers. This makes the results of the Market Watch experts’ investigation even more alarming,” says Kai Vogel, head of Unit Healthcare at the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband, vzbv). In order to make better decisions about if and how to use wearables and fitness apps, consumers need hard and fast facts about proven benefits of the services and about how their personal data will be handled. Vogel calls for “a public, nation-wide consumer information online platform to tackle these issues by providing high-quality health information and independent evaluations of digital products.”

Vzbv also shares consumers’ concerns in dealing with data collected about their levels of fitness. “We categorically reject the concept of coupling health insurance premiums with a persistent, permanent duty to share data,” emphasises Vogel, seeing a very high risk that these kinds of insurance schemes would undermine the principle of solidarity in the German health care system. “The current principle is that young and healthy insurees finance care for their older and less healthy counterparts. As soon as health insurers have enough data to start calculating individual risk, however, this above-mentioned basic principle will be scrapped. Those who suffer from diseases and feeble health should not face punishment for their situation,” concludes Vogel.

Additional information

Cease and desist orders:
- VZ NRW has sent cease and desist orders regarding breaches of privacy law to the following nine providers of mobile health and fitness services: Apple, Garmin, Fitbit, Jawbone, Polar, Runtastic, Striiv, UnderArmour (MyFitnessPal), Withings.

Methodology:
- Examinations were carried out of twelve wearable devices and the matching fitness apps available for the iOS and Android operating systems in the period of the investigation (01/07-11/08/2016). The devices’ Bluetooth connections and the way the apps store and transmit data were tested. All testing was carried out by datenschutz nord GmbH.
- The results of the consumer survey are based on a representative telephone survey of 1055 people over 14 years of age who used the internet at some point in the last three months. The survey was carried out between 25/08 and 29/09/2016 by mindline media GmbH (margin of error of whole sample: max. +/-3 % at a share of 50%).
- 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.
About vzbv’s Market Watch Digital World: vzbv’s Market Watch Digital World is a dedicated early warning and market monitoring system providing both the Federation of German Consumer Organisations (vzbv) and each of the regional Consumer Associations individually with a consumer perspective of developments in the digital sphere. The work builds on consumer complaints, representative studies, and an interactive online platform; the Market Watch Digital World can also support monitoring and regulatory bodies such as the Federal Network Agency (Bundesnetzagentur, BNetzA) in their work. Five Consumer Associations are part of Market Watch Digital World and scrutinise specific aspects of the digital market: Bavaria – digital services; Brandenburg – purchasing of digital goods; North-Rhine-Westphalia – user-generated content; Rhineland Palatinate – digital products; and Schleswig Holstein – telecommunications services. The project receives funding from the German Federal Ministry of Justice and Consumer Protection (Bundesministerium der Justiz und für Verbraucherschutz, BMJV).

http://www.marktwaechter.de/digitalewelt

Your contact for further information

Andrea Wiehager | Editorial officer (Market Watch Digital World)
Verbraucherzentrale Nordrhein-Westfalen e.V.
Tel. +49 (0)211 / 3809-405
andrea.wiehager@verbraucherzentrale.nrw

Timo Beyer | Press and public relations officer (Market Watch brief)
Verbraucherzentrale Bundesverband e.V. (vzbv)
Tel. +49 (0)30 / 25800-529
timo.beyer@vzbv.de