

New report finds health wearable devices pose new consumer and privacy risks

December 15 2016

Personal health wearable devices used to monitor heart rates, sleep patterns, calories, and even stress levels raise new privacy and security risks, according to a report released today by researchers at American University and the Center for Digital Democracy. Watches, fitness bands, and so-called "smart" clothing, linked to apps and mobile devices, are part of a growing "connected-health" system in the U.S., promising to provide people with more efficient ways to manage their own health.

The report, *Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection*, found that the weak and fragmented [health](#)-privacy regulatory system fails to provide adequate federal laws to safeguard [personal health](#) information collected by wearables. The report provides an overview and analysis of the major features, key players, and trends that are shaping the new consumer-wearable and connected-health marketplace.

"Many of these devices are already being integrated into a growing Big Data digital health and marketing ecosystem, which is focused on gathering and monetizing personal and [health data](#) in order to influence consumer behavior," the report explains. As the use of these devices becomes more widespread, and as their functionalities become increasingly sophisticated, "the extent and nature of [data collection](#) will be unprecedented."

The report documents a number of current digital health marketing practices that threaten the privacy of consumer health information,

including "condition targeting," "look-alike modeling," predictive analytics, "scoring," and the real-time buying and selling of individual consumers. The technology of wearable devices makes them particularly powerful tools for data collection and digital marketing.

The report also explains how an emerging set of techniques and Big-Data practices are being developed to harness the unique capabilities of wearables—such as biosensors that track bodily functions, and "haptic technology" that enables users to "feel" actual body sensations. Pharmaceutical companies are poised to be among the major beneficiaries of wearable marketing.

The report offers suggestions for how government, industry, philanthropy, nonprofit organizations, and academic institutions can work together to develop a comprehensive approach to health privacy and consumer protection in the era of Big Data and the Internet of Things. These include:

- Clear, enforceable standards for both the collection and use of information;
- Formal processes for assessing the benefits and risks of data use; and
- Stronger regulation of direct-to-consumer marketing by pharmaceutical companies.

"The connected-health system is still in an early, fluid stage of development," explained Kathryn C. Montgomery, Professor of Communication with American University, and a co-author of the report. "There is an urgent need to build meaningful, effective, and enforceable safeguards into its foundation."

Such efforts "will require moving beyond the traditional focus on protecting individual privacy, and extending safeguards to cover a range

of broader societal goals, such as ensuring fairness, preventing discrimination, and promoting equity," the report says.

"In the wake of the recent election, the United States is on the eve of a major public debate over the future of its health-care system," the report notes. "The potential of personal digital devices to reduce health-care spending will likely play an important role," as lawmakers deliberate the fate of the Affordable Care Act. However, unless there are adequate regulatory safeguards in place, "consumers and patients could face serious risks to their privacy and security, and also be subjected to discrimination and other harms."

"Americans now face a growing loss of their most sensitive information, as their health data are collected and analyzed on a continuous basis, combined with information about their finances, ethnicity, location, and online and off-line behaviors," said Jeff Chester, Executive Director of the Center for Digital Democracy, also a co-author of the report. "Policy makers must act decisively to protect consumers in today's Big Data era."

The three authors of the [report](#) —Kathryn Montgomery, Jeff Chester, and Katharina Kopp—have played a leading role on digital privacy issues, and were responsible for the campaign during the 1990s that led to enactment by Congress of the Children's Online Privacy Protection Act (COPPA).

Provided by American University

Citation: New report finds health wearable devices pose new consumer and privacy risks (2016, December 15) retrieved 24 April 2024 from <https://phys.org/news/2016-12-health-wearable-devices-pose-consumer.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.