April 6, 2017

Dear GBCC Teams,

Enclosed you will find the case for the 2017 Global Business Case Competition ***"Fitbit: The Business About Wrist."***

Fitbit CEO James Park has invited you to a meeting. You represent a variety of functions at Fitbit. Here is what he tells you:

> *I have just finished reading a news report about privacy risks in the wearables market [article attached]. I have also been seeing a lot of news about security risks – how data from fitness devices can be hacked when it is transmitted and stored. I have been reading reports like these for a while, and I think it is time for us directly address these issues. As I always say, we are a software and services company, not just a hardware company. Software and services will continue to be a key differentiator in our industry. How we deal with privacy and security issues can be part of what will differentiate us in the future.*
>
> *I am designating you as an ad hoc strategy team. I want you to come back on Saturday and recommend a plan for us to get out ahead of our competitors in addressing the privacy and security aspects of data protection. I also want you to suggest how we can market this new approach to our customers.*
>
> *Remember that we are counting on global markets for much of our future growth. I am particularly concerned with satisfying the new data protection laws in the EU, and I am worried about falling revenue in the Asia-Pacific region. I also want you to take into account general market conditions for wrist-wearable devices, our competitive position, our company's financial constraints, and changing technology.*

Competition Guidelines & Rules

Obviously, you will need to do outside research in order to prepare your presentation. However, you may not conduct any personal interviews as part of that research. For example, do not call, visit, or e-mail anyone at the case company. The only sources that you may use are publicly available ones (print or electronic). Please note that you are allowed to ask librarians where reference materials are located, but not for help on your research strategy.

Do not discuss the case, your research, or your presentation with anyone outside your team (this includes your advisor, your ambassador, and GBCC managers) before Saturday's competition.

If you have a question about the competition, the rules, these instructions or the case, contact Angela Shelley (angelajs@uw.edu or 307-996-7418).

I look forward to seeing your presentations on Saturday. Have fun!

Sincerely,

Debra Glassman, Faculty Director, Global Business Center

Enclosures: Article A: New report finds health wearable devices pose new consumer and privacy risks

Article A

US Official News

December 15, 2016 Thursday

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

LENGTH: 789 words

DATELINE: New York

Washington: American Association for the Advancement of Science has issued the following news release:

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).