Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection

Kathryn C. Montgomery, PhD, American University
Jeff Chester, MSW, Center for Digital Democracy
Katharina Kopp, PhD, Center for Digital Democracy

CENTER FOR DIGITAL DEMOCRACY

SCHOOL *of* COMMUNICATION
AMERICAN UNIVERSITY • WASHINGTON, DC

Executive Summary

EXECUTIVE SUMMARY

Today's consumers are embracing a new generation of mobile apps, bracelets, watches, and biosensor-equipped clothing that promise to help them lose weight, get into better shape, and reduce stress. With hundreds of these new digital tools now on the market, wearable devices have moved from a niche product just a few years ago to an expanding mass-market category. This growth has been spurred by several factors, including the widespread adoption of smartphones, the growing reliance on digital media for health information and services, and the rise of the so-called "quantified-self movement."

Health-monitoring tools are helping patients remember to take their medications regularly and reducing the number of times they need to see their doctors. Public-health and medical researchers are employing wearable cameras and other mobile devices to analyze real-world physical activity and sedentary behavior patterns among certain populations, tapping into a much wider range of data than they could through traditional methods of sampling and recruitment. Wearable devices are expected to be particularly beneficial for under-served communities and individuals with serious, chronic health problems.

But some of the very features that make mobile and wearable devices so promising also raise serious concerns. As their use becomes more widespread, and as their functionalities become even more sophisticated, the extent and nature of data collection will be unprecedented. Biosensors will routinely be able to capture not only an individual's heart rate, body temperature, and movement, but also brain activity, moods, and emotions. These data can, in turn, be combined with personal information from other sources—including health-care providers and drug companies—raising such potential harms as discriminatory profiling, manipulative marketing, and security breaches.

This 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. Its goal is to develop an informed approach to considering the best policies for ensuring equity, privacy, and security. These issues are a microcosm of a much broader and deeper set of concerns about risks to consumers in the Big-Data era. Our research is drawn from a variety of sources, including interviews with industry, privacy, health, and technology experts; analysis of industry reports, trade publications, and policy documents; participation in conferences and workshops; and review of relevant scholarly and legal literature.

We begin by taking a broad look at how the U.S. health-care system is currently being reconfigured. This transformation is fueled by a number of technological, social, legislative, and economic forces that have recently come into play:

Advances in technology and data science, including consumer adoption of mobile apps and devices, and new developments in machine learning and data analytics;

Federal requirements and incentives that are fostering the adoption of electronic health records;

Interest in new forms of lower-cost treatment by health facilities, including the use of mobile services;

Investment by venture capitalists, as well as by leading technology companies such as Google, Apple, and Intel, in new services and health-related consumer devices;

Reimbursement by Medicare and other health insurance providers for new digitally based health services, such as remote diagnostics; and

Growing numbers of start-ups and new competitors offering health and insurance services that are tied to various forms of digital technology.

EXECUTIVE SUMMARY

The growth of connected health is further eroding the boundaries between the health-care system and the digital commercial marketplace.

The technology of wearable devices makes them particularly powerful tools for data collection and digital marketing. A new generation of techniques will likely become defining features of the user experience in the emerging wearables environment. Many will be extensions of contemporary digital marketing practices currently in use. For example, smartphones and other mobile devices already provide unprecedented access to users' location information, enabling marketers to target individuals wherever they are, based on analyses of "visitation patterns" and a host of other behavioral and demographic data. An emerging set of techniques will be designed 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.

Experts envision a not-too-distant future in which health and wellness devices—along with an array of next-generation Internet-connected sensors—will be fully integrated into everyday experiences as people continue to adapt to the now-ubiquitous presence of digital technology in their lives. The flow of user-generated and biologically derived information that these devices track will be fed through a vast Big-Data network composed of hospitals, pharmaceutical companies, consumer product goods and services companies, drugstores, and many other players both within and outside the increasingly porous connected-health system. Algorithmic classification systems could enable profiling and discrimination—based on ethnicity, age, gender, medical condition, and other information—across a spectrum of fields, such as employment, education, insurance, finance, criminal justice, and social services, affecting not only individuals but also groups and society at large. The opportunities for data breaches will increase, with hackers accessing medical and health information at insurance companies, retail chains, and other businesses. Even those institutions with the most benevolent of goals—such as public-health departments, law enforcement, and research entities—can misappropriate and misuse health data. Many of the harms associated with the collection and processing of such data, moreover, are likely to affect disproportionately the most vulnerable people in our society, including the sickest, the poorest, and those with the least education.

The degree to which users of wearable devices will be able to make informed privacy decisions—and thus exercise meaningful control over their personal data—will ultimately depend on the effectiveness of government and self-regulatory policies. In their current state, however, none of these systems provides adequate safeguards to patients or consumers in the Big-Data era. In contrast to the European Union, where privacy is encoded in law as a fundamental right and where robust data-protection laws have been enacted, privacy regulation in the U.S. is sectorial, with separate laws for different types of information, users, and situations, such as financial, student, or medical privacy. Overall, U.S. privacy laws governing health information are limited and fragmented, with significant gaps in coverage. Although there have been efforts over the years to pass broader consumer-privacy regulations in the U.S., none has been successful.

Trade groups and industry-supported nonprofits have developed guidelines, codes of conduct, principles, and best practices for addressing privacy and marketing in digital media. Taken together, these self-regulatory regimes offer a patchwork

EXECUTIVE SUMMARY

of competing and sometimes overlapping systems. While claiming to give consumers tools for controlling their own personal data, many of the actual practices are often described in such vague, complex, or highly technical language that they are difficult to comprehend. Nor do self-regulatory systems offer any meaningful system of independent accountability.

Privacy, security, and consumer-protection policies for the connected-health market should be held to a much higher standard than those established for most other areas of the digital marketplace. Addressing these concerns requires a comprehensive framework that will ensure true accountability and enable effective enforcement. If policies can be put in place now, consumers will have legitimate reasons to trust the companies with which they do business, and will gain confidence in the fairness of the overall consumer marketplace. Rather than stifling innovation, these policies will both foster and guide the growth of the industry.

A first principle that too often gets lost in the complicated and technical inside-the-beltway policy discourse is that privacy needs to be considered not just a preference, but rather a fundamental and inalienable right. If this basic right is the bedrock of a revised and strengthened national privacy policy in the Big-Data era—for consumer protection generally and for health privacy in particular—six other vitally important issues must be addressed in turn:

The need for twenty-first-century Big-Data safeguards: For decades, privacy and data-protection policies—in both Europe and the U.S., as well as in many other countries—have been guided by Fair Information Practices, sometimes called Fair Information Practice Principles (FIPPs). FIPPs are considered the gold standard of privacy policy, a framework that combines a set of rights for individuals with a clear articulation of responsibilities to govern how institutions can collect and use personal data. The underlying conflict between traditional privacy principles and Big-Data imperatives, however, has prompted some to declare that FIPPs are simply no longer relevant. But rather than abandoning FIPPs, we need to strengthen and supplement these longstanding principles, developing additional standards and practices that can address a host of new and emerging data operations. This will require moving beyond the 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.

Moving beyond privacy self-management: The prevailing model of *notice and choice*—which has been embraced by both government regulators and industry—operates on the assumption that an individual will review the disclosures in a company's privacy policy, evaluate the pros and cons for herself, and, if she uses or purchases the product or service, will agree to the terms of the data-processing arrangement. Such expectations of "privacy self-management," however, are at odds with contemporary Big-Data practices.

Improving transparency: Meaningful and effective transparency is consistent with the FIPPs principle of openness. However, current corporate privacy disclosure practices fail to explain the full spectrum of data collection, sharing, and marketing techniques employed on wearable devices, leaving a great deal of room for improvement. Transparency, moreover, needs to go beyond corporate privacy policies and terms of service. The pervasive use of algorithms in many sectors of our society—including social media, marketing, science, and government—has triggered rising concern about how these "black box" operations can negatively impact individuals, communities, and groups.

Redefining "protected data": Both regulatory agencies and industry self-regulatory organizations classify certain kinds of information as "sensitive" and thus deserving

EXECUTIVE SUMMARY

of greater privacy protection. While personal health information should clearly be considered sensitive, it is important to understand that in the Big-Data era, no single piece of data or category of information can easily be isolated for special handling. We need to view current data practices more holistically, as the aggregation of many "data points" about an individual, across multiple platforms and digital devices, online and off, that reveals important and "actionable" insights about a person's health. Restricted categories of so-called personally identifiable information (PII) are also problematic and outmoded in today's digital marketing environment.

Limiting collection and regulating use: Policy makers should consider establishing more effective ways to assess both the benefits and risks of data use—not only to individuals, but also to groups and the larger society. Data-technology practices should be required to undergo some form of risk-impact assessment before they are put in place. While industry self-regulatory organizations can play a role in this process of risk-impact assessment, risk/benefit analysis, and the establishment of acceptable data-use categories and risk levels, they should not be the sole arbiters of decision making in any of these areas.

The need for new regulatory structures: While we need to do everything possible to educate and empower consumers to take control of their personal data, we cannot expect individuals to bear the entire burden of managing their privacy in the Big-Data era. Privacy advocates have long been arguing for the establishment of a data-protection authority to replace our current fragmented structure of privacy regulation in the U.S. Given the widespread and transformative nature of data-driven operations and practices across multiple sectors of our society, an overarching regulatory structure may be necessary to manage a broad spectrum of issues, ensuring ethical data-processing practices, instituting effective consumer-privacy safeguards, and preventing discriminatory uses of data.

Establishing effective safeguards for the wearables and connected-health marketplace will require widespread participation across many sectors of our society, including the high-tech and health industries, academic institutions, nonprofits, foundations, policy makers, and communities. This report concludes with a number of suggested next steps. These include efforts to strengthen public interest and nonprofit participation in health-privacy reform; to promote public education on the need for such reform; to develop a collaborative and cross-cutting research agenda; and to foster stronger industry safeguards and best practices. Because contemporary marketplace practices pose challenges to effective decision making by individuals, the report proposes a set of principles designed to give consumers as much control as possible over their own data, while establishing default safeguards for both collection and use.

***All* data collected** from a health or wellness wearable device should be considered sensitive, and thus require an affirmative and effective consent process before they can be collected and used.

Clear, enforceable standards should be established for both the *collection* and *use* of information on wearables and other Internet-connected devices, with allowances for consumers to place limits on the data collected by and about them.

Companies should be required to explain fully and in clear language what their data practices are, and there should be standardization of terminology so that

EXECUTIVE SUMMARY

comparisons are possible. They should also be required to make public disclosures about the operations of their data-analytic systems, including how they conceptualize and utilize algorithms.

Wearable and other connected-health companies should not share user information with any third parties where advertising, marketing, or the promotion of other services are involved.

Companies should comply with requests for a person's data as soon as possible and at the lowest cost.

The metrics used to determine how de-identification is most effectively accomplished should be disclosed and subject to independent verification.

In order to ensure that consumers are truly informed, wearable devices and apps should be tested to determine that consumers will be able to *understand* their privacy choices and terms of services.

Self-regulatory organizations should develop standards that apply to *all* sectors of the consumer connected-health industry, along with a process for independent auditing.

The various participants in the digital health sector, including the wearable and mobile apps industry, should develop a set of fair marketing practices for using health-related data.

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 Affordable Care Act is very likely to undergo significant transformation, with millions of Americans facing the prospect of losing their health insurance or having their coverage severely cut. The potential of personal digital devices to reduce health care spending will likely play an important role in the policy debate. However, as this report documents, these technologies hold both promise and peril. In the absence of adequate safeguards, consumers and patients could face serious risks to their privacy and security, and also be subjected to discrimination and other harms. We have both an unprecedented opportunity and a moral obligation to broaden our national conversation around the goal of establishing a "Culture of Health," where "good health and well-being flourish across geographic, demographic, and social sectors," and "everyone has the opportunity to make choices that lead to healthy lifestyles."

Table of Contents

Introduction

One of the featured products at the 2016 Consumer Electronics Show (CES) was Under Armour's new "UA Record app," a powerful personal health tool that monitors and analyzes a person's behavioral and performance data gathered by a fitness-tracking device. Billed as "the world's first 24/7 connected health and fitness system," UA Record promises its users their own "personal health consultant, fitness trainer and assistant," utilizing IBM's Watson artificial intelligence computing system to "assess and combine" an array of personal, physiological, nutrition, training, and environmental information. The app also taps into Under Armour's 160-million-member "Connected Fitness" community.[1]

UA Record is one of hundreds of new digital tools on the market to help people improve their health and well-being. (See sidebar: "Wearable Market Players.") Through smart-phone apps, bracelets, watches, and biosensor-equipped clothing, consumers are increasingly eager to embrace technology that promises to help them lose weight, get into better shape, reduce stress, and take more control of their health. Digital strategy firm Endeavour Partners explained in a recent report that "smart wearable devices have moved from a niche product just a few years ago to a mass-market product category."[2] This growth has been spurred by several factors, including the widespread adoption of smart phones, the growing reliance on digital media for health information and services, and the rise of the so-called "quantified-self movement."[3] It is estimated that more than 500 million consumers with smartphones worldwide have downloaded health apps to their devices. The global market for mobile health services is projected to reach $49.12 billion by 2020, up from $1.95 billion in 2012. 232 million wearable devices were sold in 2015, with U.S. consumers in the forefront of purchasing watchers and fitness trackers.[4] Health and fitness devices are now getting less expensive, making broader adoption by the public likely.[5]

Takeaways from "The Internet of Me", released by Ericsson[1]

Wearable ownership almost doubled in the past year;

24% of new users of wearables are aged 15-24;

Two out of five users described themselves as feeling 'naked' if they didn't wear their device for a day

The following are just a few highlights of products and new ventures in this fast-moving consumer health device marketplace:

Samsung has designed a "Bio-Processor" for its fitness apps, which will be able to measure a combination of bodily processes and states, including body fat, skeletal muscle mass, heart rate, heart rhythm, skin temperature, and stress level.[6]

Fitbit is one of a number of companies developing the next generation of wearable tools that will piece together different biometrics, including sleep patterns, heart rate, and galvanic skin response. The device will send consumers warnings of stress levels and suggest ways to reduce stress.[7]

Apple released its Apple Watch in 2015, with health and fitness offerings among its suite of bundled apps. The Health app on Apple Watch "measures all the ways you move, such as walking the dog, taking the stairs, or playing with your kids. It even keeps track of when you stand up and encourages you to keep moving."[8] For the broader app-development community, the company also released HealthKit, which "allows apps that provide health and fitness services to share their data with the new Health app and with each other. A user's health information is stored in a centralized and secure location and the user decides which data should be shared with your app."[9]

A start-up called Thync "uses neuroscience to provide a clean way to manage your energy, stress, and sleep.... Thync uses low-energy waveforms to safely and comfortably signal nerves on your head and face. These nerves signal specific areas of the brain that cause your body to relax or energize."[10] The company says it is the first consumer wearable device that is marketed to improve a person's mood.[11]

CONNECTED HEALTH IN THE BIG-DATA ERA

Wearables are expected to play a central role in a new "connected-health" system. "Increasingly, people are gathering data from their own bodies, tracking outcomes, and sharing information with colleagues and friends," explains a recent article in the journal *Health Affairs*. "Patient-consumers," empowered by technology, have "access to real-time, actionable, and personal information," not only enabling them to make better decisions about their own health, but also generating valuable data for broader public health interventions: "Devices such as Jawbone UP, Fitbit, NikeFuel, and others track one's daily steps, sleep habits, and nutrition. Other apps broadcast exercise stats and favorite running routes to friends. Online communities invite patients to share tips, drug side effects, and prayers—all while big analytic engines comb through the findings in a constant search for unexpected determinants of healthy behavior."[12]

The emergence of wearables is emblematic of the Big-Data era. Advances in computer technology, artificial intelligence, digital communication networks, and sophisticated data-processing and analysis tools have triggered a sea change in the amount, speed, and variety of data that can be gathered and processed. The costs of collecting, storing, and processing data have gone down as the sources for gathering data have proliferated. The forces of Big Data are reshaping all of the major institutions in our society, disrupting the structures and operations of government, commerce, health, financial markets, education, and the workplace.[13]

THE INTERNET OF WEARABLE THINGS

Wearables are also part of the rapidly growing Internet of Things, in which Internet-connected sensors transform the ordinary objects in peoples' everyday lives—from thermostats to refrigerators to cars—into "smart" devices that can communicate with each other.[14] Technology company Ericsson recently released a report on the "Internet of Me," which offered several illustrations of some of the wearables available in the near future. For example, "wearable panic buttons" could be "built into jewelry or clothing, allowing you to quickly alert a pre-designated circle of trusted contacts, as well as the police, when in distress." "Safe driving internables" might include "ingestible pills with sensors, which measure blood alcohol content" and "communicate with your car, rendering it useless if you exceed the legal limit."[15] A report from Cisco's Internet of Everything center describes a world in which "people will be able to swallow a pill that senses and reports the health of their digestive tract to a doctor over a secure Internet connection," and where "sensors placed on the skin or sewn into clothing will provide information about a person's vital signs."[16] Google is already developing a digital contact lens that could transform medical care for diabetes by measuring blood glucose levels from an individual's tears.[17]

If harnessed effectively, this growing array of fitness trackers, smart-phone apps, and other Internet-connected devices could help address some of the most challenging public health problems in the United States. Wearables are already proving to be useful tools for reducing health-care costs and increasing patient engagement, and could play a role in addressing the dramatic rise in obesity over the last several decades, which has triggered an increase in type 2 diabetes, heart disease, and other related illnesses. Health-monitoring tools provide individuals with more efficient ways to manage their own health, encouraging them to take their medications regularly and reducing the number of times they need to see their doctors.[18] Dozens of companies are incorporating health and fitness trackers into their employee-wellness programs.[19] (See sidebar: "Employee Wellness Programs.") Public health and medical researchers are using wearable cameras and other mobile tools to analyze real-world physical activity and sedentary

CONTINUED ON PAGE 14 →

Wearable Market Players

The connected-health and fitness-device market is composed of several competing sectors, including leading digital technology firms Apple, Google, and Samsung; specialized companies that focus on technological tools, such as Garmin and Misfit; and fitness-focused entities, such as Under Armour and Adidas. Consumer wearable devices already offer an array of health-related data.[2] In addition to the number of steps taken, heart rate, distance walked, blood pressure, and sleep patterns, products can also display email, send text messages, trigger payments at the store, deliver notifications, and connect to social media.[3] Among the leading wearable device companies are the following:

Fitbit: Claiming it has "the largest community of connected health and fitness device usaers," the company offers a number of "wearable connected health trackers" that connect to a person's wrist or can be clipped to their clothing, such as the Fitbit Zip, Fitbit Charge, and Fitbit Blaze. As customers use its data platform, Fitbit says it gains a "deeper understanding" of their "health and fitness goals" and is positioned to develop a "direct relationship" with them—offering "analysis, features, advice, and content...throughout the day...." Customers can be reached when they use "our online dashboard, mobile apps, emails, and notifications." There are also "thousands of third-party apps" with which a Fitbit customer can decide to share data.[4]

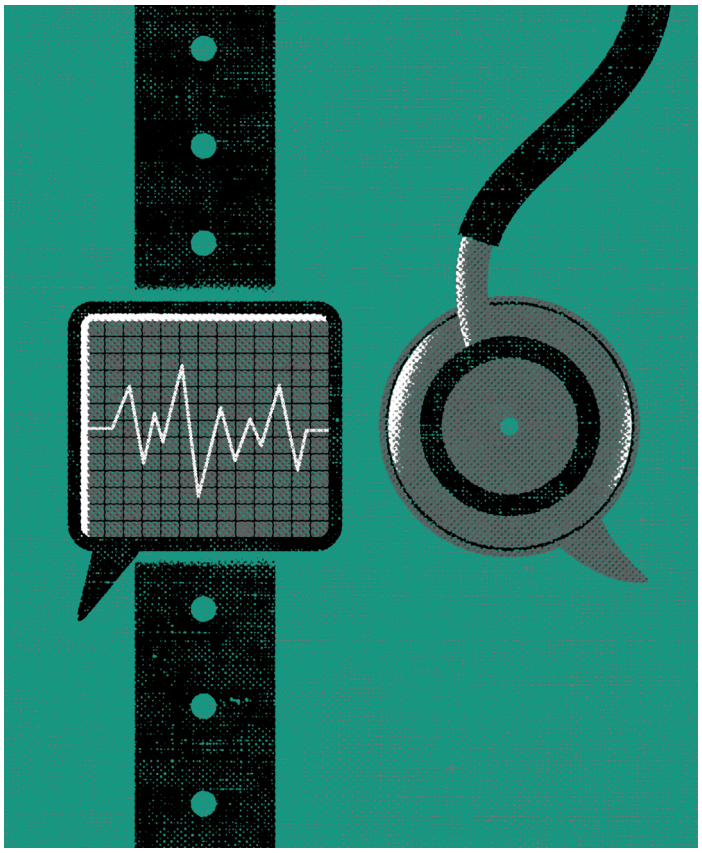
Fossil Group: The "fashion and technology" company acquired Misfit, maker of activity trackers and smartwatches, in late 2015. Like others, Fossil is focused on building out its ability to provide digitally delivered services to its customers, including through its use of data. Among its product line are the Ray, Bolt, and Shine. Misfit is also working to sell its devices to healthcare companies and employee-benefit plans.

Garmin: In addition to consumer sales, Garmin aims as well to sell its watches and trackers to employee-wellness programs. With this device, users can receive "smart notifications" through "email, call, text, social media alerts and more—all from your wrist."

Under Armour: Initially known for its line of sports apparel, Under Armour now also offers a variety of wearables and digital fitness services.[5] The company's "connected-fitness" platform includes apps, such as Endomondo and MyFitnessPal, that provide activity, diet, and other information. Through its UA Record, for example, Under Armour says it "collects and analyzes data points from all your digital devices," offering a personalized dashboard and the ability to "coach you on your next workout," among other features.[6]

Samsung: The electronics giant manufacturers smart watches and fitness bands, and has focused on mobile health-care applications for its line of mobile phones. Its "S Health" app works with the sensors in Samsung phones that can provide "complete integrated solutions to patient recovery and wellness." In addition to tracking calories used, activity level, and ultraviolet light exposure, Samsung mobile devices can become "a precise chronic disease management solutions" and a monitor for diabetes, blood pressure, and cardiac issues.[7]

The leading operating systems for smart watches are Apple's watchOS, with nearly two-thirds of the global market, and Google's Android Wear (which has slightly more than 20 percent).[8] The future direction of wearables is being shaped by the ability of marketers to use behavioral information gathered in real time. They will offer more personalized messages and promotions as they are "directly accessing pulse rate, sweat levels, and even scanning facial expressions...."[9]



behavior patterns among certain populations, tapping into a much wider spectrum of data than what is possible through traditional methods of sampling and recruitment.[20] Wearable devices could be particularly useful for under-served communities and individuals with serious, chronic health problems.[21]

WEARABLES' THREAT TO PRIVACY

But some of the very features that make mobile and wearable devices so promising also raise serious concerns. Because of their capacity to collect and use large amounts of personal data—and, in particular, sensitive health data—this new generation of digital tools brings with it a host of privacy, security, and other risks. Many of these devices are already being integrated into a growing digital health and marketing ecosystem, which is focused on gathering and monetizing personal and health data in order to influence consumer behavior. As the use of trackers, smart watches, Internet-connected clothing, and other wearables becomes more widespread, and as their functionalities become even more sophisticated, the extent and nature of data collection will be unprecedented. Biosensors will routinely be able to capture not only an individual's heart rate, body temperature, and movement, but also brain activity, moods, and emotions. These data can, in turn, be combined with personal information from other sources—including health-care providers and drug companies—raising such potential harms as discriminatory profiling, manipulative marketing, and data breaches. According to the Health and Human Services' Office of Civil Rights (OCR), there were 253 health-care breaches in 2015 that affected 500 individuals or more, resulting in a combined loss of over 112 million records.[22]

Yet mobile health apps and wearable devices currently fall between the cracks of an already weak and fragmented health-privacy regulatory system in the U.S. Many consumers may think that their personal health information is protected by federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA). But that law applies only to medical facilities, insurance companies, pharmacies, and other so-called "covered entities," and there are many loopholes in the system that allow patient data to be used by a growing spectrum of companies and institutions.[23] While some wearables, such as those prescribed by doctors,

CONTINUED ON PAGE 16 →

Increasingly, people are gathering data from their own bodies, tracking outcomes, and sharing information with colleagues and friends

Employee Wellness Programs

Obesity-related illnesses are costing American businesses $73.1 billion per year in medical expenses and lost productivity.[10] According to the National Institutes of Health (NIH), more than two out of three adults are either overweight or obese. And more than 1 in 20 (6.3 percent) are considered extremely obese.[11]

Retail giant Target recently teamed up with Fitbit to encourage its 335,000 U.S. workers to engage in healthier behaviors. Those who enrolled in the program were given free or discounted Fitbit activity trackers and organized into teams for a month-long "Activity Challenge." The team that logged the highest average number of daily steps was given $1 million to distribute to their favorite local health and wellness nonprofit groups.[12] And while there hasn't been a great deal of research on the topic, a number of major companies report that using these devices has made a clear difference in how well workers respond to wellness initiatives. When IBM distributed Fitbits to 40,000 employees over a two-year period, 96 percent of them logged their health information, such as physical activity and food intake, on a routine basis, and many continued to wear the trackers months after the company challenge was over.[13]

Wearables will increasingly play a role in the emerging "medical device information system" that gathers, analyzes and distributes health data. Such combined information will help provide, according to a Qualcomm subsidiary, a "comprehensive view" of a patient. UnitedHealthcare, a major health services company, in partnership with Qualcomm, now offers a program for employers that provides wearable devices to employees and dependents. The devices, which are designed to help employees and their families "become healthier and more active" connects to a "medical grade data" network (and enables remote monitoring by health professionals, for example). Employees who participate and wear the devices can earn credits, up to $1,450 per year for their health reimbursement accounts.[14]

In October 2016, AARP filed a lawsuit against the Equal Employment Opportunity Commission (EEOC), charging that the federal agency's forthcoming rules for wellness programs would "penalize workers for keeping health information private." The EEOC's plan, which starts in 2017, allows employers to offer financial incentives to those who sign up for their wellness plans, amounting to as much as 30 percent off of what an employee pays annually for insurance. AARP is worried that the new policy will force many employees and their families to provide their health information to corporate wellness services.[15]

INTRODUCTION

might fall under the jurisdiction of the Food and Drug Administration (FDA), which regulates the use of medical devices, many of the most popular health and fitness devices and mobile apps are consumer products that the FDA does not regulate. The Federal Trade Commission (FTC) has some authority over mobile apps and Internet-enabled devices, but its regulatory jurisdiction is limited. Trade associations and industry-supported policy organizations have begun developing voluntary codes of good practice that health-technology companies may adopt to provide assurances to users that their data are safe. However, at the critical point when this market is about to take off, there is no government or self-regulatory framework that adequately addresses the privacy and consumer-protection issues raised by wearable health devices.[24]

Some of the most important stakeholders in the policy arena are still largely uninformed about the nature and extent of data collection in the emerging wearables industry, its relationship to the broader health and technology sector, and the stakes involved. Developments are moving forward at such breakneck speed across a range of health-related areas that it is difficult for most people to comprehend their full scope and dimensions, or understand the complex set of issues they raise.

Though the market is still in an early stage of development, it is possible to identify the forces that are shaping it, its major features, and key players, in order to develop an informed approach to considering the best policies for ensuring privacy, security, and equity. The research for this report is drawn from a variety of sources, including interviews with industry, privacy, health, and technology experts; analysis of industry reports, trade publications, and policy documents; participation in conferences and workshops; and review of relevant scholarly and legal literature.[25] Our focus is primarily on the consumer wearables and mobile marketplace, which we define broadly to encompass smart clothing, fitness trackers, mobile apps, and similar tools.

The issues raised by health wearables are a microcosm of much broader and deeper concerns about the growing risks to privacy in the Big-Data era. We hope this report will contribute to a national discussion among consumers, health professionals, policy makers, industry, and the public at large.

We have organized the remainder of this report into five sections:

CHAPTER 1:

We begin by identifying several key trends that are influencing the growth and direction of the wearables market, including the emergence and expansion of an increasingly seamless, integrated connected-health system, spurred by government initiatives and fueled by large infusions of investment capital. PG 18

CHAPTER 2:

We then provide an overview of the current health and privacy regulatory landscape in the U.S., identifying some of the critical gaps in coverage as well as the challenges posed by contemporary data-driven commercial practices. PG 36

CHAPTER 3:

This is followed by a brief description and assessment of the key self-regulatory systems for data collection and marketing in the digital media, mobile, and wearables industries. PG 42

CHAPTER 4:

In the next section, we highlight what we see as the most important principles and issues that need to be considered in order to establish a public-interest framework for the health and wearables marketplace. PG 48

CHAPTER 5:

Lastly, we suggest ways in which government, industry, philanthropy, nonprofit organizations, and academic institutions can work together to develop a comprehensive approach to privacy and consumer protection, highlighting key principles, best practices, and recommended next steps. PG 66

CHAPTER 1:

Wearables and the Changing Health Marketplace

To understand the wearables and mobile health app marketplace, we need to take a broad look at several key trends that are reshaping the U.S. healthcare system:

- federal government policies promoting the growth of information technology in health and medical care;
- major financial investments by venture capitalists and leading online companies in a new generation of digital health services and consumer devices; and
- Big-Data precision medicine initiatives that encourage public-private partnerships in order to generate breakthroughs for disease treatment and prevention.

FEDERAL HEALTH INITIATIVES

U.S. policymakers have enacted a series of federal initiatives designed to promote greater health and wellbeing, address inefficiencies in our current medical system, lower costs, and contribute to improvements in outcomes. In all of them, information technology (IT) plays a central role. For example, the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH) created a new Office of the National Coordinator for Health Information Technology (ONC) within the Department of Health and Human Services (HHS), which is mandated to promote "the empowerment of individuals to improve their health and health care through Health IT." A key goal of the HITECH Act is the development of a "learning health system" that supports the needs of both individuals and providers, and fosters continuous improvements for quality outcomes. It also envisions an IT infrastructure "where an individual's health information is not limited to what is stored in electronic health records, but includes information from many sources (including technologies that individuals use) and portrays a longitudinal picture of their health…[and] where public health agencies and researchers can rapidly learn, develop, and deliver cutting edge treatments."[26] The Affordable Care Act (ACA), which was enacted in 2010, includes provisions for promoting the adoption of electronic health records by medical professionals and enabling patients to gain easier access to their own data. ACA also encourages more effective use of data to improve evaluation and outcomes.[27]

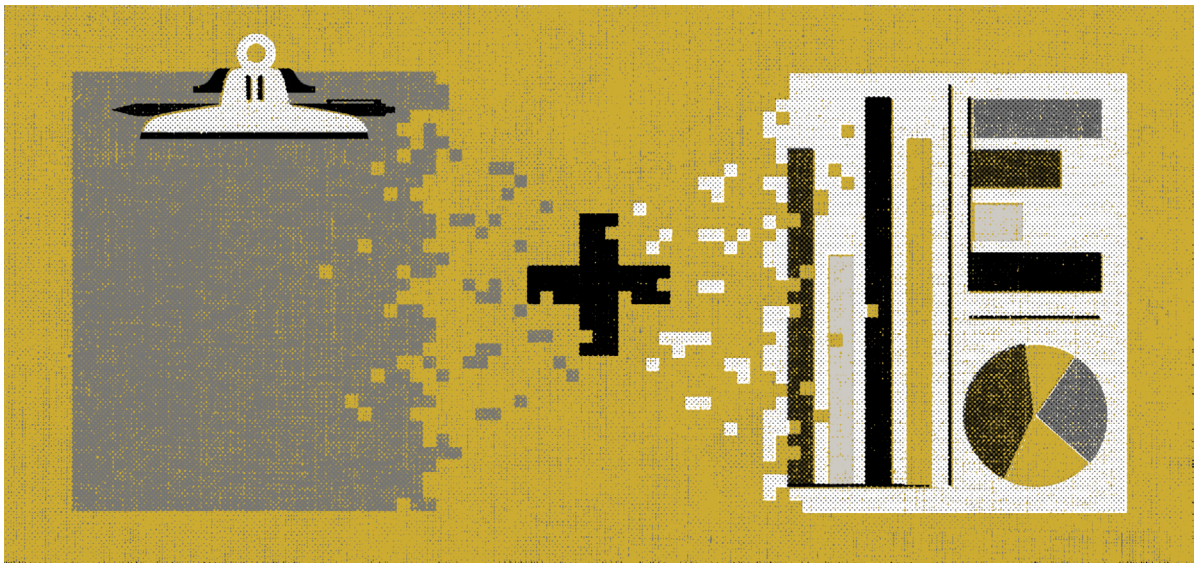
WEARABLES AND THE CHANGING HEALTH MARKETPLACE

INVESTMENT IN DIGITAL HEALTH SERVICES

The venture-investment community is also playing a significant role in fueling the growth of this connected-health system. Medical technology companies have attracted major funding for a broad array of innovations and new digital ventures designed to streamline and reconfigure conventional health and medical operations. For 2014 and 2015, more than $4 billion was invested each year in the "digital health space." The top sectors financed provide insight into the changes occurring in the health system: health-care consumer engagement; wearables and bio-sensing consumer devices; personal health tools; payer administration tools for handling health-care transactions; telemedicine services that include digital imaging and videoconferencing; and care coordination. Investors understand the significant financial rewards to be made by creating state-of-the-art health services and applications, including those that take advantage of the availability of personal health data. Google Ventures (now GV), which invests in "early-stage" start-ups, has contributed 30 percent of its annual funding to health companies, for example.[28] As one of its partners explained, "We are looking at the intersection of where data science and healthcare meet, (which can include) everything from primary care to devices to patients."[29] There were also significant connected-health merger and acquisition transactions in 2015, "with 180 deals and $6 billion in disclosed activity." Five digital health IPOs, including Fitbit's, created $9 billion in market capitalization.[30]

BIG DATA AND PRECISION MEDICINE

The federal government has been promoting the growth of precision medicine, which



relies heavily on Big-Data technologies and systems to identify individual differences in environments, genes, and lifestyles in order to develop both personalized and large-scale approaches to disease prevention and treatment. The White House's Precision Medicine Initiative (PMI) was launched in 2015 to support "emerging methods for managing and analyzing large data sets while protecting privacy, and health information technology to accelerate biomedical discoveries." A "million or more Americans" are to be asked to "volunteer to contribute their health data," in order to "catalyze a new era of data-based and more precise medical treatment." Key principles include making "it easier for patients to access, understand and share their own digital health data, including donating it for research" and "open[ing] up data and technology tools to invite citizen participation, unleash new discoveries, and bring together diverse collaborators...."[31] Earlier this year, the White House announced the creation of a new Cancer Moonshot Task Force—to be led by Vice President Joe Biden—which is aimed at accelerating cancer treatment research and development. The initiative will foster data sharing in order to "break down barriers between institutions, including those in the public and private sectors, to enable maximum knowledge gained and patients helped."[32]

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

A number of public and nonprofit health and research institutions are partnering with private, for-profit technology companies to develop large-scale medical research efforts. For example, Google is making investments in the use of data-related practices to create "the world's largest single source of structured real-world oncology data and intelligence."[33] Its health-focused research unit, Verily (formerly Google Life Sciences), was launched in 2015 and is working on a variety of projects, including wearables for diabetes and multiple sclerosis, "medical robots," and studies on nanodiagnostics. Verily has formed partnerships with pharmaceutical companies Novartis, Dexcom, and Sanofi for products related to diabetes; with Biogen on multiple sclerosis; and with Johnson and Johnson on robots.[34] In one of the first PMI-funded projects, Verily is also collaborating with Vanderbilt University to enroll volunteers who will share their health data for research.[35]

As a recent PricewaterhouseCoopers report explained, all of these trends have created a "New Health Economy," which

is altering traditional business models: "The industry's very value chain is being re-engineered by powerful global drivers—downward pressure on costs, increasing chronic diseases, an aging population, surging consumerism, the embrace of value-based models, the arrival of new entrants and, yes, transformative advances in technology."[36]

GROWTH AND MATURATION OF THE BIG-DATA DIGITAL MARKETPLACE

The growth of this new health economy is further eroding the boundaries between the health-care system and the digital commercial marketplace. Since its origins in the mid-1990s, the digital marketing system has operated with a core business model that relies on continuous data collection and monitoring of individual online behavior patterns.[37] Now well established and thriving, its expenditures reached nearly $60 billion in 2015 for the U.S. alone, with worldwide spending predicted to reach $285 billion by 2020.[38] The integration of data collection and marketing has become even deeper in the Big-Data era, with the proliferation of digital platforms and devices, innovations in online measurement techniques, and the growth of data analytics.[39] An expanding arsenal of software and analytic tools are enhancing the ability of digital media companies and their advertisers to glean valuable insights from the oceans of data they generate.[40] An elaborate and pervasive system can track and analyze a complex range of behaviors, actions, and networked relationships taking place online and offline, and increasingly on mobile devices.[41] These developments have created what some observers have called the "surveillance economy."[42]

The technological affordances of wearables make them particularly powerful tools for both extensive data collection and personalized marketing. According to a recent survey conducted for a leading digital e-commerce marketing firm, the "key benefit

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

of wearables will be as a source of very granular data insights and also new types of behavioral and usage data. Wearables of the future will have the ability to capture a wide array of data related to a user's contextual activity, health and emotional state." More than a third of marketers surveyed want to capture "daily routine and precise location" information from these devices. Smart watches are considered an additional "screen" that can be added to today's cross-screen marketing system, which has grown exponentially over the last several years.[43] Market research conducted for a leading digital ad company predicts that wearables will join with other connected devices to provide "an increasingly rich view of the consumer." In the emerging Internet of Things environment, they will work alongside smartphones, tablets, connected TVs, medical appliances, connected cars, and the "multiple embedded touchpoints" increasingly found in homes and communities.[44]

THE MOVE TO DIGITALLY-DIRECT-TO-CONSUMER PHARMACEUTICAL MARKETING

Pharmaceutical companies are poised to be among the major beneficiaries of wearable marketing, along with a number of other players in the growing digital and connected-health system. The U.S. and New Zealand are the only two developed countries that permit direct-to-consumer (DTC) advertising of pharmaceutical products.[45] (See sidebar: "Digital Direct to Consumer Drug and Health Marketing.") Spending for DTC advertising has skyrocketed in recent years to more than $4.5 billion.[46] While the bulk of these expenditures has been for television commercials, pharmaceutical companies have moved aggressively into digital media, as a more cost-effective way of targeting and engaging consumers.[47] The U.S. health-care and pharmaceutical industry is expected to spend $1.93 billion on digital advertising in 2016, up more than 15 percent from the previous year.[48] By 2020, forecasts online marketing research firm eMarketer, pharmaceutical and health digital ad spending will reach $3.10 billion.[49]

CONTINUED ON PAGE 23 →

Digital Direct to Consumer Drug and Health Marketing

The Food and Drug Administration (FDA) and the Federal Trade Commission (FTC) are responsible for overseeing the advertising and marketing of prescription medications and over-the-counter drugs, respectively. The FDA's over-arching framework for the advertising and promotion of pharmaceuticals and other regulated medical products is that they "must be truthful, accurately communicated, and balanced in presenting a drug's risks and benefits" (or "fair balance"). These rules are designed to prevent "false and misleading" pharmaceutical advertising, and to ensure such ads reflect known risks of using a particular drug.[16]

The FDA's primary work on digital advertising has been to ensure that benefit-and-risk information is available, on search engines, social media, and blogs. It also has made clear that companies that operate their own social media services are responsible for identifying and responding to information related to potential harmful impacts of their products.[17] In addition, the FDA provides guidance on how companies should handle online services that have "character space limitations" (such as Twitter) so they can provide adequate "fair balance" information. Despite the space limitations, the most serious concerns must be identified, the FDA explains. Companies are allowed to provide a "more complete discussion" of the risks and benefits of a drug through the provision of a hyperlink on a search or microblogging site.[18]

The American Medical Association (AMA) called for a "Ban on Direct to Consumer Advertising of Prescription Drugs and Medical Devices" in a new policy adopted in 2015. The AMA's then-incoming president explained that direct to consumer (DTC) advertising plays a harmful role by promoting "expensive treatments" versus clinically proven "less costly alternatives." Dr. Patricia Harris noted that DTC advertising "inflates demand for new and more expensive drugs, even when these drugs may not be appropriate." The AMA policy also reflects a concern about the growing "anticompetitive behavior in a consolidated pharmaceutical marketplace" and its impact on affordable medications.[19]

Big Data is at the heart of today's pharmaceutical marketing efforts. "Every decision we make today is fueled by data, and it's changing the way we buy [ads]," explains the group president of Publicis Health and Razorfish Health—part of the second-largest global ad agency. Digital advertising provides "measureable results," agrees the president of SSCG Media Group, another leading pharma marketing firm, which is why "media budgets are shifting to include more channels and targeting opportunities than ever before to engage both healthcare providers and patients." In addition to recognizing that people are online today (with overall spending for digital ads expected to outpace TV expenditures in 2017), there is another economic reality confronting the pharma industry. "As the era of blockbuster drugs comes to an end," explains eMarketer, "many prescription drugs in the pipeline will cater to diseases with specific remedies.... [T]hey will require more highly targeted campaigns and strategic use of digital channels."[50] Pharmaceutical companies are responding to these challenges through various approaches, including partnerships, new ventures, and additional personnel.[51]

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

"HIPAA-compliant" has become a term of art for a growing set of techniques drawn from the Big-Data digital marketing arsenal

While pharmaceutical marketing is federally regulated, the industry has been able to engage in robust advertising and promotion efforts, which will become even more sophisticated in the next few years. For example, regulations that the FDA administers—including adverse-event-notification requirements and those affecting endorsements and promotion—have historically constrained the willingness and ability of pharmaceutical companies to fully deploy digital marketing techniques. However, there is clear evidence that these companies are beginning to push back against limitations that may have restricted them in the past.[52] In addition to the FDA regulations, HIPAA includes a Privacy Rule that prohibits hospitals, doctors' offices, and other covered entities from using an individual's personal health information for marketing purposes without that person's prior authorization. However, the definition of what is considered "marketing" includes a number of exceptions. Though passage of the HITECH Act in 2009, along with subsequent HHS rules, has closed some of the loopholes, there are still a number of ways in which covered entities, their business associates, and third parties can engage in marketing practices.[53] In the pharmaceutical marketing industry, "HIPAA-compliant" has become a term of art for a growing set of techniques drawn from the Big-Data digital marketing arsenal.[54]

In their new jointly authored book, *Pharma 3D: Rewriting the Script of Marketing in the Digital Age*, representatives from Wharton, McKinsey, and Google urge the pharmaceutical industry to "think in 3D" and take advantage of the "moments that matter to their customers' decision-making," including "both patients and providers."[55] The book's many recommendations offer a blueprint of Big-Data digital marketing technologies and practices that have already been eagerly embraced by the food and beverage, financial, retail, and other industries. The book also lays out a "CareFlow" framework that maps how, through digital marketing, "pharma leaders find a more compelling role to play in the lives of their patients, prescribers, and all others who influence patient behaviors and decisions." The authors explain that

> Discovery in the Digital Age is the art of combining numeric and emotional views of behavior across the CareFlow. As such, it is not simply classic data mining or even "big data" number crunching that many think of when discussing business intelligence. The Digital Age Discover process recognizes that the data are coming from new sources; for example, we ourselves are often the sources of

data, whether from our medical records or the Fitbits and smart watches around our wrists. Effective discovery, therefore, requires a perpetual "insights engine," one that never stops combining these torrents of data with ethnographic and attitudinal insights.[56]

Wearable devices "can lead to unique patient insights and engagement…broaden patient engagement beyond treatment initiation and ultimately build manufacturer and brand loyalty," the book explains. "[A]s consumers continue to collect more activity and health data and become more comfortable with how companies handle private information, they are increasingly willing to share these data with healthcare players in order to improve outcomes or reduce costs."[57]

Wearables and mobile apps figure prominently in the pharmaceutical industry's strategy for engaging smaller, niche markets with highly focused advertising. "[T]he payoff is still a few years away," according to the Publicis Health president. But companies are examining how to "leverage the different things that people are tracking—

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

steps, sleeping, daily insulin measures—and provide them services throughout their journey that may go beyond our drugs."[58] With consumer health and wellness data continually merged into profiles alongside financial, location, purchase, and social data and other information, marketers now possess the ability to track and reach individuals anytime and anywhere, with data-driven marketing technologies that create "actionable" insights for influencing a person's behavior. Health-related marketing applications will potentially be integrated with a consumer's daily use of financial payment and other online applications. Powered by sophisticated technologies, such as IBM's "Watson" cognitive computing system, apps are able to provide individuals with health information "unique to them."[59]

THE EMERGING WEARABLES DATA-COLLECTION AND MARKETING SYSTEM

The advertising industry is gearing up to take advantage of wearables and other digital devices for data-driven targeted marketing, developing advanced data collection,

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

analytics, and delivery capabilities, drawing from recent innovations in behavioral science, and launching ad networks and other new ventures targeted exclusively to this segment.[60] For example, leading ad agency Mindshare (Group M/WPP) created a "wearable technology unit" in 2014 called Life+.[61] Under Armour's "Connected Fitness" advertising network enables targeting users of its health-related apps, including MyFitness Pal, MapMyFitness, and Endomondo (a personal-training app).[62] FitAd, another new fitness and health mobile ad network, offers targeting via "the largest possible targeted audience for fitness & health," involving such user data as "ethnicity, age, gender, location, [and] browser data."lxiii Ad agencies and data-targeting companies are actively exploring a variety of ways to harness the capabilities of these new devices on behalf of their clients.[64] There is interest in "tying offline data to online behaviors and connecting medical and clinical data with nonmedical behavioral and demographic information to infer and predict health behavior and conditions."[65]

With consumer health and wellness data merged into profiles alongside other information, marketers now possess the ability to track and reach individuals anytime and anywhere

A start-up called Strap bills itself as "the most efficient way to use mobile health data." Its founders "realized that there was a need for someone to analyze and make sense of the data coming from the growing number of wearable devices."[66] The company offers a "HIPAA-compliant mHealth analytics platform" that can deliver "actionable insights" from more that 200 wearables and devices that enable "access to hundreds of millions of users and their data." As consumers opt in, "human data starts flowing into Strap's intelligence system," enabling marketers to "send messages around the time your consumers wake up, reward them for reaching fitness goals and know what kinds of food they eat regularly.... By using this data to your advantage, you can encourage them to be more loyal consumers with rewards, coupons and freebies." Strap is able to "couple human data" with a client's information, including loyalty, social media, shopper, and survey data.[67]

According to a recent eMarketer article, "advertising will not appear in volume on wearables until one or more of the devices attains significant market share." But as soon as these new devices reach mass adoption, "advertisers expect to connect with users through native ad formats."[68] In the parlance of the ad industry, "native ad formats" are the latest form of product placement, the practice of blending advertising and brands seamlessly into website and mobile app content so that consumers cannot tell the difference. One health marketer notes that "native advertising formats are becoming the preferred mode of engaging with brand and disease information," especially since they bypass ad blockers and are not perceived as ads.[69] On wearable devices, native advertising will take a number of forms. For example, "native newsfeed sponsorships" may deliver "an organic brand message to consumers as they view nutrition and fitness content and community support from trusted friends and family."[70] Native ads can also be interactive experiences, using video to blend into the editorial content. For example, FitAd specializes in delivering what it calls "moments":

> Moments mark the start, completion or achievement of an important milestone within a fitness and health app or website. At these Moments, it is appropriate to match advertising to the Moment so that brands can acknowledge, recognize, reward or challenge users. Examples of Moments include: beginning a run, descending a mountain, driving for your longest golf shot, beating your best 5k time, or simply making a healthy food or lifestyle choice that is being captured via an app or webs.[71]

Native ads are just one of a variety of data-collection practices and targeting techniques that will likely become defining features of the user experience in the emerging wearables environment. Many of these techniques will be extensions of contemporary Big-Data digital marketing practices currently in use on mobile and other platforms, adapted to take full advantage of the unique capacities of wearables and their role in consumers' daily lives. Others will be tailored specifically to the wearable marketplace, harnessing new capabilities such as biosensors that track bodily functions and "haptic technology" that enables users to "feel" actual body sensations.[72] In the next few pages, we highlight some of these practices, explaining how they work and providing examples of their current use by health and pharmaceutical marketers, as well as how they will likely be deployed in the wearables market.

PREDICTIVE ANALYTICS AND BEHAVIORAL TARGETING

The last several years have witnessed a proliferation of specialized services offering a variety of Big-Data services to marketers. Among these are data-management platforms and data marketing clouds, which provide a package of complex, sophisticated computer operations that are already central features of contemporary digital marketing. (See sidebar: "Data Management Platforms and Health Marketing Clouds.") For example, *predictive analytics* involves collecting data on a consumer's behaviors and other attributes from a variety of sources, combining that data with profiles of the individual, and using sophisticated algorithms to distill and interpret the data in order to make predictions about how that person is likely to respond to a given marketing message. Through *behavioral profiling and targeting,* the specific message and its distribution can be precisely tailored and targeted to maximize its ability to influence that particular consumer.[73]

IMS Health, which operates a data-management platform and cloud-computing service for health marketers, recommends

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

that its clients gather behavioral and profile data from all of the "stakeholders" in the "healthcare ecosystem," including "the healthcare professional, the pharmacist, the patient, the payer, the provider, the thought leader, and others," in order to analyze and influence the "patient journey." Using "insight-driven, automation-enabled marketing" to "construct communications journeys," a "series of messages sent to healthcare professionals and patients are tailored and iteratively refined to be more effective."[74] "Iteratively refined" refers to a common practice in the digital marketing industry whereby messages can be altered in real-time based on a consumer's reactions, and further adjusted for maximum effect. Through this practice, sometimes called *dynamic creative,* the enhanced message can be retargeted to the same individual as she navigates the Web or uses a mobile device.[75] "Targeting customers as individuals is achievable," explains IMS, "once you collect data on their past behavior, attitudes and preferences."[76]

Wearables are expected to play a major role in dramatically increasing the availability of behavioral data on individual consumers, resulting in what one IMS executive referred to as a "wave of information coming our way."[77] A growing number of companies now specialize in offering data services specifically tailored to the mobile health and wearables industry. For example, Validic describes itself as "the healthcare industry's premier technology platform for convenient, easy access to digital health data from best-in-class clinical and remote-monitoring devices, sensors, fitness equipment, wearables and patient wellness applications."[78] Validic has access to "patient data from over 280 application and devices," with a "population reach of 223 million throughout 27 countries." Its partners include RunKeeper, Misfit, Fitbit, Pfizer, along with health-marketing-supported information companies WebMD and Everyday Health. In June 2016, Validic partnered with leading global ad giant Omnicom "to counsel healthcare companies on the connected health market and to develop new solutions that integrate data from wearables, apps and clinical remote monitoring devices."[79]

CONTINUED ON PAGE 28 →

Data-Management Platforms and Health Marketing Clouds

Data-management platforms (DMPs) are one of many new entities involved in data-driven digital marketing.

These services provide marketers with "centralized control of all of their audience and campaign data."[20] They do this by collecting and analyzing data about individuals from a wide variety of online and offline sources. This encompasses several levels of data categories: so-called "first-party data," which comes from a customer's own record, such as the use of a supermarket loyalty card, or their activities captured on a website, mobile phone, or wearable device; "second-party data," which is information collected about a person by another company, such as an online publisher, and sold to others; and "third-party data," which is drawn from thousands of sources, and can include demographic, financial, and other data-broker information, including race, ethnicity, and presence of children.[21] All of this information can be matched to create highly granular "target audience segments" and to identify and target individuals "across third party ad networks and exchanges." DMPs also "measure with accuracy which campaigns perform the best across segments and channels to refine media buys and ad creative over time."[22]

Developed by well-known companies such as Adobe, Oracle, Salesforce, Nielsen, and IBM, data marketing clouds are a one-stop shopping service, enabling marketers to integrate scores of different sources of consumer information about online and offline behaviors. There are a number of marketing clouds focused on the health market. These health marketing clouds offer practically unlimited access to health data that can be combined with consumer financial, health, family, and other information. Marketers can mix and match these data to build powerful profiles that can be used to target consumers in real time, whether on their mobile device or computer.[23] For example, the Oracle Marketing Cloud for Life Sciences provides pharmaceutical and health services companies a hub that "allows companies to break through data, brand, and functional silos to provide a 360-degree view of their marketing efforts...reaching a company's optimal consumers across all marketing channels." Oracle tells its health clients that it can help them "unify" their data to target the "right customers," deliver "individualized" marketing content ("dynamic targeting and segmentation") "across all channels" (such as Web, mobile, social, and email), and measure the results.[24]

IMS Health's Nexxus Commercial Application Suite provides "cloud-based applications for healthcare and life sciences that integrate sales and marketing activities across the ecosystem." Its "IMS One Intelligent Cloud" integrates information from patients, pharmacists, insurance companies, and medical providers to help deliver multichannel marketing, sales, and other services. "Orchestrated Customer Engagement" (OCE), explains IMS, goes beyond targeting consumers and health professionals on all their devices and communications channels. With OCE, "sales, marketing and information technology are closely aligned," with "near real time" integration of all the data available to help generate "predictive" insights.[25]

"SCORING," "PERSONAS," AND "LOOKALIKE MODELING"

Predictive analytics have helped usher in an expanded set of tools for *scoring,* rating, and categorizing individuals, based on an increasingly granular set of behavioral, demographic, and psychographic data. For example, Adobe's Marketing Cloud offers marketers the ability to rate individual consumers on the basis of their "digital body language and their behavior." From these inferences, each consumer can be assigned a *persona* corresponding to a framework adapted from psychologist "[Abraham] Maslow's hierarchy of needs."[80] Another health-marketing specialist, Crossix, has devised its own "Consumer Database Scoring solution," which uses "predictive Rx and OTC data to improve segmentation, so you can customize outbound messaging, optimize communication cadence and more." The company has also created "actionable profiles" that are "based on the modeled relationships between health behaviors and consumer attributes."[81]

Through *lookalike modeling,* companies are able to acquire information about an individual without directly observing behavior or obtaining consent. They do this by "cloning" their "most valuable customers" in order to identify and target other prospective individuals for marketing purposes.[82] The following is an explanation of the practice from eXelate, a data-marketing company owned by Nielsen:

> Lookalike modeling is a process that draws on advertisers' understanding of what the online behavior of their best customers entails. Once these characteristics are identified, third-party data providers then match these profiles or "personas" with likely effective, prospective audience data sets leveraged from pools of modeling data available online. Marketers can then approach these prospects with relevant digital messaging that achieves better reach and retargeting.[83]

Health and pharmaceutical marketers often use lookalike modeling to identify and target individuals who have a strong likelihood of being concerned about (or at risk for) a particular disease or medical condition. This is done by analyzing the behaviors of those people known to have, or to be at risk for, the disease, and then matching these detailed models with profiles of others in third-party databases, individuals who may not be associated with the disease but who exhibit the same set of behaviors as people who are.[84]

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

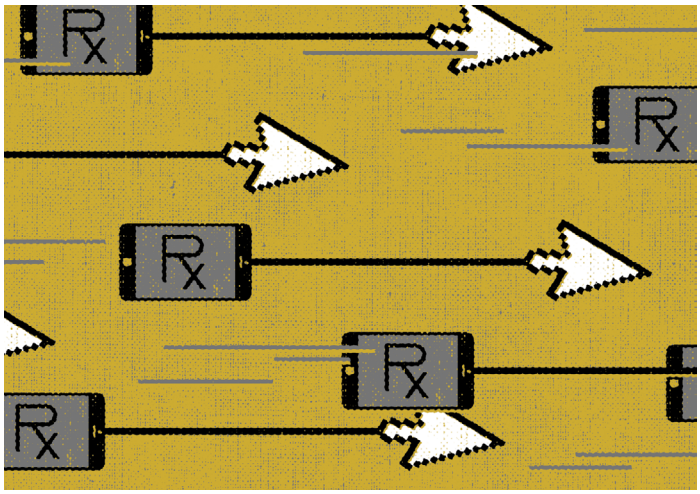
Data-marketing firms assure their clients that all of these classification and targeting tools are "HIPAA-compliant." As Crossix's promotional materials explain, for example, "At no time is an individual's actual health data used in the application of the models for media targeting purposes."[85] However, it is clear that the use of Big-Data technologies and operations have made it possible for health marketers to determine—with an unprecedented degree of precision—an individual's health status, risk level, propensity to disease, and medical concerns, and to identify, locate, and target that person, without ever needing access to any medical records.

These practices are already being adapted for use with wearable devices. For example, Skyhook, a mobile-location digital marketing company, has developed personas, as part of its AdTech product line, to enable targeting of individuals who share similar characteristics or concerns, based on data points that include ethnicity, location, demographic, and behavioral data.[86]

CONDITION TARGETING

Similar practices are frequently employed by pharmaceutical companies and other health marketers to target individuals based on a particular disease or medical condition. So-called *condition targeting* has become a mainstay for the drug industry, enhanced and expanded in the digital era. The advertising network Adprime, for example, offers targeting of consumers based on such health issues as cancer, diabetes, heart disease, HIV/AIDS, mental health, and sleeping disorders. The company provides behavioral and script

targeting services (based on analyses of prescription drug sales), where marketers can reach "patients by treatment and diagnosis."[87] Another health-marketing company, AdRx Media, which is owned by leading data firm Conversant, offers its clients targeting built upon "data from millions of anonymous online profiles," promising to provide access to users with the following conditions: allergies, asthma and respiratory conditions, cancer, cold and flu symptoms, diabetes, digestive health, heart disease, joint health, mental health, osteoporosis,



severe headaches and migraines, sexual health, sleep disorders, weight management, and more.[88]

Condition targeting also taps into the growing number of online searches by consumers seeking health information. More than 70 percent of consumers now rely on online media, including mobile devices, to inform themselves about health concerns. Forty percent of those individuals "directly act" after they obtain online health information. One in twenty Google searches involves health. Nearly 50 percent of consumers search for reviews and other information on physicians.[89] African Americans and Latinos are more likely than whites to use their mobile phones to search for health information.[90]

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

Consumers are also increasingly turning to social media and online videos to seek health information and connect to individuals and groups with a similar concern or interest about a condition or product. Many of the most popular health-information services also provide their advertisers and corporate sponsors, such as pharmaceutical companies, with the latest digital marketing tools. For example, Vertical Health, which offers online health information on chronic pain, diabetes, thyroid conditions, mental health, and medications, and which counts major pharmaceutical brands among its clients, partners with leading providers and facilitators of online targeting, including Acxiom, AppNexus, Merkle, and Underscore.[91] Healthline, "the fastest growing consumer health information" site, recently received $95 million in equity funding to help it expand. With 22 million U.S. users every month, Healthline "offers medically reviewed clinical content that is authoritative, approachable and actionable." Its partners include drugs.com, livestrong.com, BlackHealthMatters.com, EmpowHER, and others. It promises "unmatched access to condition-specific Facebook communities," tracking consumers when they go to Facebook from one of its sites.[92]

Fitness apps and wearable devices are already integrated into the health-information marketplace. The "primary driver" of growth for the popular health-information site WebMD is now consumers using mobile devices to access its services. Its WebMD for the iPhone application offers a "health improvement program" that it calls "Healthy Targets." The app gathers a person's biometric data from activity trackers, glucose meters, wireless scales, and blood-pressure monitors.[93]

PROGRAMMATIC MARKETING

One of many terms in the digital marketing industry that means something quite different from what it would appear to mean, programmatic marketing has nothing to do with advertising on television programs. Rather, it refers to new automated forms of ad buying and placement on digital media using

computer programs (thus "programmatic") and algorithmic processes to find and target a customer wherever she goes. The process can also involve real-time "auctions" that occur in milliseconds in order to "show an ad to a specific customer, in a specific context." Many in the industry see programmatic marketing as the future of advertising, and it is already in use within the pharmaceutical and health sectors.[94]

Ad giant Publicis's health division launched a "programmatic platform" in 2014 called AOD Health. Publicis represents approximately 200 "health and wellness brands," including pharmaceuticals and over-the-counter medications. The company says that it has access to "two big buckets" of health and user-related data in order to "identify and target audiences," and to "back-end sources" that can optimize and measure an ad's impact. Such data give it "real-time insights" for its planning and "activation" teams, and are being used, for example, to reach out to "niche audiences" for more specialized drugs that do not have a large market.[95] Another company now using programmatic targeting is Everyday Health, a provider of "digital health and wellness solutions" that owns or operates websites, mobile apps, and social media services, including Dr. Sanjay Gupta, Physician's Desk Reference, pregnancy and parenting site What to Expect, and MayoClinic Diet. (It also partners with MayoClinic.org).[96] Its marketing division, known as "Health Reach," provides programmatic targeting opportunities through the use of consumer registration information compiled from Everyday Health sites. "Consumer Profiles" are constructed that enable advertisers to track and target consumers wherever they go "outside of [the] Everyday Health portfolio." Health Reach says it provides a "cost-effective online audience targeting solution that efficiently connects pharmaceutical and OTC brands to valuable, condition-specific audiences at scale." It claims to have access to data from the "largest condition-specific audience on the Internet," which is mingled with "user activity data" from search engines and social media, and also incorporates information provided by "35 online data aggregators."[97]

Programmatic targeting for mobile devices has also grown in sophistication, and can combine data on an individual or demographic (cookie-based, offline data, purchase data, ethnicity, age, etc.), analyze "where people go"—physical world (location) data—and take advantage of a mobile device's identifiers.[98] Programmatic marketing relies on technologies that track and target consumers across many different digital platforms. Through a process of "cross-device recognition," marketers can determine if the same person who is on a social network is also using a personal computer and later watching video on a mobile phone. Another recent marketing technology breakthrough is the ability to transform (the industry term is "onboard") offline data into digital data-targeting profiles—such as cookies or mobile-device identifiers—to make advertising more personal and relevant.[99] The practice facilitates differential treatment of various categories of consumers based on behavioral profile information. For example, some individuals will be offered rewards, discounts, or information; others might be viewed as having a low lifetime-revenue potential and given less favorable treatment or ignored entirely.[100]

GEOLOCATION AND GEO-MEDICAL TARGETING

Mobile devices continually send signals that enable advertisers (and others) to take advantage of an individual's location—through the phone's GPS (global positioning system), Wi-Fi, and Bluetooth communications. All of this can be done with increasing speed and efficiency. Online marketers have determined that, on average, people check their phones 150 times a day, and that 87 percent have such devices with them all day long, even while they sleep.[101] Through a host of new location-targeting technologies, consumers can now be identified and targeted wherever they go, while driving a car, pulling into a mall, or shopping in a store.[102] A complex and growing infrastructure of geolocation-based data-marketing services has emerged, with specialized mobile data firms,

machine-learning technologies, measurement companies, and new technical standards to facilitate on-the-go targeting.[103] Google and Facebook, which often know the actual ("authenticated") identity of their consumers, have expanded their use of location for ad targeting.[104]

FitAd's "mobile and wearable advertising platform" delivers targeted advertising to a "mobile audience of 50 million people, creating over 1 billion monthly screen views." The data collection, targeting, and analytics features of its "PrecisionTap" system facilitate precise targeting based on a wide spectrum of demographic, socioeconomic, lifestyle, and location factors, including ethnicity, gender, age, household income, and ZIP code. Advertisers can target via five classes of "inventory"—"mind, body, life, sports and outdoor, and fuel"—to promote not only fitness and health brands, but also pharmaceuticals, amusement parks, and alcoholic beverages.[105]

An entire industry has been developed to identify the characteristics of the places people visit—called "place data"—generating new insights to help companies more precisely reach their prospects.[106] Place data can include the characteristics of a particular neighborhood, such as its ethnic/racial mix and income level, along with customer information from loyalty programs and online tracking.[107] Neighborhoods and communities across the country have been digitally "sliced and diced" through the use of mapping and database software, creating geo-data-rich profiles.[108] As consumers enter specific areas they can pass through a "geo-fence"—an invisible online perimeter that triggers ads and coupons to be delivered via mobile devices.[109]

In the pharmaceutical and health sector, "geo-medical targeting" enables marketers to identify "highly concentrated areas of the country where diagnosed patients live" or where prescriptions for certain kinds of drugs are frequently written. Geo-medical marketers also use "HIPAA-compliant" medical and prescription-use information through the acquisition of "de-identified insurance claim data for patient diagnostic intelligence," as well as data from area pharmacies. Such information, say digital pharma experts, powers geo-medical targeting to transform "direct to consumer advertising" into "direct to patient advertising."[110] Geo-medical strategies reach beyond individual patients or consumers to involve a network of online health-service partners that provide information to both consumers and physicians. For example, one geo-medical marketing company works with "leading healthcare professional societies, associations, [and] consumer health sites," including the American Academy of Family Physicians, American Diabetes Association, American Gastroenterological Association, the "Glucose Buddy" mobile app, FamilyDoctor.org, and many others. "Channels" are available to target consumer concerns about heart health, mental health, HIV/Aids, diabetes, and conditions related to "women and mothers."[111]

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

CONTEXTUAL HYPERTARGETING

Pharma companies are also using *hypertargeting* techniques to reach and engage consumers when they are viewing particular kinds of content online or on their mobile phones (described as "contextual targeting on steroids"). Using programmatic, real-time data-exchange operations, marketers can reach individuals "at the most ideal time because the consumer is actively engaged with the topic at hand."[112] One hypertargeting company, PageScience, for example, "delivers targeted branding to patients as they research symptoms across hundreds of premium sites before and after their doctor visit." Through its "PageMatch," the company "scores 100 million pages a week and continuously ranks pages across premium domains in a proprietary data warehouse. It provides continuous data on availability by physical condition."[113] Pharmaceutical marketers engaged in hypertargeting claim that the practice protects privacy because it does not involve the use of cookies to identify and track individuals. However, their promotional materials also claim that it is "more effective and precise than cookie targeting."[114]

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

HYPER-TARGETED MOBILE MARKETING

Hyper-targeted mobile marketing is expanding into doctor's offices, as part of an emerging "point-of-care" strategy that is comparable to "point-of-sale" digital marketing of consumer goods in the retail industry.[115] *Beacons,* small devices that send signals to individual mobile phones in close range, are being used for the "delivery of dynamic, data-driven, and relevant mobile engagement experiences for patients and advertisers...." The Health Media Network (HMN) is "one of the fastest growing digital Point of Care media companies in the U.S., providing education and health content in physician waiting rooms."[116] HMN is now deploying beacons at more than 12,000 provider locations, enabling pharmaceutical marketers, consumer packaged goods, and other health-oriented products and services to "leverage the power of targeted messaging to patients during a critical window of time in their health journey." The company also offers a "multicultural network" to target African Americans and Hispanics, as well as specialized networks for "new moms," seniors, women, and individuals with a variety of conditions (oncology, neurology, diabetes, HIV, pain).[117]

The leading U.S pharmacy chains have expanded their use of digital marketing techniques to reach and engage customers and to tap into new sources of data

RETAIL PHARMACY DIGITAL MARKETING

In recent years, retail drug chains have moved more centrally into the health-delivery business, opening walk-in clinics and hiring medical staff to administer vaccinations, diagnose illnesses, and educate patients on a range of health and wellness conditions.[118] As increasingly important hubs for medical care, services, and products, pharmacies are well positioned to be on the front lines of new digital marketing strategies. Along with other retailers, drugstore chains recognize that the widespread adoption of mobile and other digital devices requires strategies that take advantage of how consumers search for products and prices online before buying. Stores are wiring with Wi-Fi and Bluetooth so they can connect to mobile devices and apps to determine a consumer's location within an aisle and deliver targeted messages. They are also beginning to install "smart shelves" and digitally enabled point-of-purchase displays. As a result, a simple tap of one's phone delivers "instant" rewards or loyalty points to customers, as shelves and even products are tagged with digital technology.[119]

The leading U.S pharmacy chains have expanded their use of digital marketing techniques to reach and engage customers and to tap into new sources of data. Health and fitness wearables figure prominently in their operations.[120] For example, Walgreens, which operates more than 8,000 retail drugstores in the 50 states, offers a "Balance Rewards" program in which customers earn points when they buy prescriptions and other products.[121] Through Walgreens' partnership with companies such as Fitbit, Jawbone, MyFitness Pal, Google Fit, and Runkeeper, customers can also be rewarded when they "track their healthy habits," such as walking, managing their weight, or monitoring their blood pressure. Walgreens has incorporated WebMD's iPhone app into the Balance Rewards program, along with WebMD's "Healthy Target" system, which enables consumers to connect their activity tracker and health devices so they can see all of their data. They can use the "symptom checker" to research conditions and medications. While "getting rewarded for making healthy choices," users also receive "WebMD contextual content and insights." Other companies that partner with the Balance Rewards program include pharmaceutical and health services companies Roche and Johnson &

Johnson, as well as game maker Atari's Fit app; Sqord, a fitness tracker for children; and Glow, a fertility tracker.[122] Walgreens works with mobile-coupon-technology company Quotient, which offers a wide range of data analytics and profiling tools to its clients.

"WEARABLE ADS" AND PERSONALIZED PUSH MESSAGES

In addition to the growing toolbox of data collection, analysis, and targeting techniques currently in use throughout the digital marketing ecosystem, wearable technologies are expected to introduce a new generation of practices designed specifically for these devices. "Wearable ads" on smartwatches are predicted to generate more than $68 million in ad revenues by 2019 (up from $1.5 million today). The appeal of targeting a person's wrist, explained Greg Ratner, head of technology at brand agency Deep Focus in New York, is that it enables "advertisers to grab consumers' attention immediately, no matter what they are doing. And it's not just about screen space. Extra sensors that collect data such as the pulse, movements and even skin temperature could help marketers better target their ads. 'Is this person awake?' 'Is that a good time to interact with that user at all, or should we wait for a different time to engage with them?' All that is just additional context to help us connect the brands with the users at the right moment."[123] "Your watch," explained a recent marketing report, "goes absolutely everywhere you do—the restroom, the gym, your morning run, shopping, and it's there even when you're sleeping. When you're on the go you may sometimes forget your phone, but it's hard to forget your watch when it's strapped to your wrist. Such rich location data is powerful for advertisers. Stores could leverage previous shopping data to prompt consumers towards a portion of the store that needs more foot traffic or is home to higher priced goods...."[124] At a recent marketing event, leading data-focused marketing-technology company Adobe projected that smart watches will be particularly effective vehicles for delivering "hyper-relevant push messages," using streaming video.[125]

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

By 2015, over 500 million of a total 1.4 billion smartphone users worldwide will be using mobile Health apps. And by 2018, 50 percent of the 3.4 billion mobile device users will have downloaded mobile Health apps. The mobile Health global market is projected to reach $49.12 billion by 2020.[26]

VIRTUAL PERSONAL "(AD)SISTANTS"

iPhone owners are already familiar with "Siri," Apple's built-in, voice-controlled virtual personal assistant, which helps users surf the Web, navigate a map, or select a piece of music to play from their iTunes app.[126] Leading digital marketers and health companies are working on a number of initiatives using artificial intelligence, deep learning, and natural-language processing to develop virtual personal assistants, designed to automate consumer decision making about which products and services to use.[127] In the wearables market, many of these commercial functionalities are likely to be merged with other health and wellness features.

Watson Ads will be able to interact with consumers while also helping marketers "uncover consumer and product insights faster than ever before"

For example, Under Armour's "UA Record" app, which was launched in 2015, incorporates a "Cognitive Coaching System" powered by IBM's Watson natural-language-processing and machine-learning system. Promising to "transform athlete engagement and motivation," the UA App will use Watson's "ability to tap into users' behavioral and performance trends tracked… [by its] mobile apps and fitness-tracking devices [and] customize programs."[128]

UA Record does not currently run ads, though other fitness apps owned by Under-Armour (including MapMyFitness) do.[129] However, it is noteworthy that the same IBM system that powers the personal coaching function on the UA Record is also being harnessed for advertising and marketing uses. In June 2016, IBM announced "Watson Ads," an "advertising solution that can create a one-to-one connection with the consumer, that can be personal, relevant and valuable; and can scale across millions of interactions and touchpoints." Watson Ads will be able to interact with consumers and answer their questions, while also helping marketers "uncover consumer and product insights faster than ever before, revealing connections previously invisible to human data scientists." GSK Consumer Healthcare is one of the first three companies working with Watson Ads (and is also part of the new Watson Ads Council). "Cognition humanizes the use of data as we move from intent-based advertising to actual one-to-one interacting," explains Theresa Agnew, CMO for GSK Consumer Healthcare. "It also gives consumers easy access to information to make better decisions about their healthcare in real time."[130]

"HAPTIC ADS" AND "EMOTION CHIPS"

Wearable devices are able to capture and use new kinds of information from consumers that were not readily accessible in the past. Biosensors can determine mood and emotional states, for example, and both respond to and trigger physical sensations through *haptic* technologies. Haptic notifications are already in use on smart watches; without looking at the watch screen, one can feel the subtle tap on the wrist signifying a phone call or text message. These capabilities offer an entire new range of marketing possibilities. "Touch is at the heart of the most powerful experiences," explains mobile ad company Immersion. Its trademarked TouchSense technology extends "the power of touch to the digital world" so that gamers can "feel the G-forces applied to a car around an S curve" and "movie watchers feel the percussion of an explosion."[131] The company also "helps brands harness the power of touch" to "create highly immersive experiences that improve engagement and profitability." By using the company's TouchSense Haptic Enabling Kit, marketers can develop "powerful brand" tactile experiences for their wearable and other device campaigns. The "Interactive Alerts Framework," explains the company, "gives you complete control over

every pulse, flutter, and tap of the device actuator." Working with data-targeting partners to deliver haptic ads, "brands can creatively connect with users, enhancing ad recall, strengthening brand impressions, and improving click-through rates."[132]

"Emotion chips," which once were confined to science fiction, are also considered one of the next frontiers of wearable digital marketing. In the near future, explained an online video from an MIT commercial spin-off, "all our devices will have an emotion chip embedded in them," a feature expected to interface particularly well with the rapidly developing Internet of Things commercial landscape. The "emotion chip would have an optical sensor and perhaps other sensors as well that can read your emotions—your facial expressions, your tone of voice, your physiology. These small chips would passively collect data about your emotional state, ...leverag[ing] machine learning on [the] device or in the cloud to make real time inferences about your emotions—for example, when a device knows that you're stressed it can modify its behavior to handle that." Marketers and others will be able to take advantage of this chip to "measure a user or crowd's emotions and respond in real time," combining it with new forms of analytics "collected on individuals' emotional responses" to "help make better decisions faster."[133]

TOWARD A FULLY INTEGRATED DIGITAL CONSUMER-HEALTH MARKETPLACE

A former executive from Oracle recently described the following scenario to illustrate how wearables will likely be integrated into people's daily lives in the coming years:

> In the future, your smartwatch will instantly access your medical records, diet and training logs, then sync them with sensors in the supermarket and mall to provide real-time shopping and health advice. Your smart shoes and biometric shirts will remind you to straighten your posture, hydrate and run and walk with correct form to protect your back and knees. A smart bandage will tell diabetics when their blood sugar is running low. Haptic technology will give you intimacy at a distance; when your wife on the phone 1,000 miles away squeezes her Fitbit, your Under Armour will tighten up.[134]

WEARABLES AND THE CHANGING HEALTH MARKETPLACE

As the connected-health marketplace continues to expand, wearables, mobile health apps, and other digital devices will interconnect with drugstore loyalty cards, mobile payments, and other commercial applications, not only co-existing but also communicating with each other on a regular basis.[135]

The same tools we use to track our activity and monitor our bodily functions will also serve as highly personalized commercial targeting systems, delivering emotional appeals that are tailored to our unique behaviors, vulnerabilities, and fears, and reaching and engaging us wherever we are or whatever we're doing, even in the most intimate of personal spaces. So, for example, when a woman steps on the scale in her bathroom, discovering to her dismay that she has gained a few pounds, her smart watch could immediately target her with a compelling and clever ad—often disguised as entertaining "content"—promoting a weight-loss drug or an interactive "bot" to serve as her personal fitness coach. Such possibilities are not as far-fetched as they may seem; they are very real extensions of current data-driven marketing practices, as consumers are increasingly targeted in grocery store aisles through their mobile phones and delivered hyper-targeted advertising near the point of purchase or through personalized billboard ads, a scenario featured in the 2002 film *Minority Report.*[136]

The degree to which users of wearable devices will be able to make informed privacy decisions—and exercise meaningful control over their personal data—will ultimately depend on the effectiveness of government and self-regulatory policies. As we explain in the following section, however, none of these systems, in their current state, provides adequate safeguards to patients or consumers in the Big-Data era.

CHAPTER 2:

Gaps and Weaknesses in Health and Privacy Regulation

During the 1970s, an era of mainframe computers, the U.S. played an important leadership role in formulating the concept of "Fair Information Practices," which was subsequently embraced and developed further by the Organization for Economic Cooperation and Development (OECD).[137] Ironically, though the U.S. led the way in articulating and promoting strong principles for protecting individual privacy—including passage of the Privacy Act of 1974, which protects people from government violation of personal privacy—it has fallen behind other countries in embracing all of those principles through laws.[138] As a consequence, observes privacy scholar Deborah Hurley, "Americans have less protection for their personal data than people in many other nations."[139]

Many of the major players involved in health marketing, such as data brokers, aggregators, ad agencies, data-management platforms, and marketing clouds, fall outside of HIPAA's coverage. Data can easily flow in and out of this HIPAA-free zone, and personal data that have been "anonymized" can be "de-anonymized easily."[143] As law professor Nicolas Terry observes, much of the information that makes up the health profile of an individual is "medically-inflected data," increasingly generated through mobile health apps, wellness devices, and connected domestic appliances. "In short," Terry explains, "big data can produce basically unprotected patient-level data that will serve as an effective proxy for HIPAA-protected data."[144] Though there is a general consensus around "health privacy exceptionalism"—that information about a person's health status deserves a higher level of privacy protection than most other information—citizens and consumers are left without effective safeguards in place.[145]

> "Big data can produce basically unprotected patient-level data that will serve as an effective proxy for HIPAA-protected data

GAPS AND WEAKNESSES IN HEALTH AND PRIVACY REGULATION

LIMITED HIPAA PROTECTIONS

In contrast to the European Union, where privacy is encoded in law as a fundamental right and where robust data-protection laws have been enacted, privacy regulation in the U.S. is sectorial, with separate laws for different types of information, users, and situations, such as financial, student, or medical privacy.[140] (See Appendix A, "Recent European Union Privacy Developments.") Privacy laws governing health information are limited and fragmented, with significant gaps in coverage.[141] For example, HIPAA's primary purpose is to ensure the flow of information throughout the health-care system. More appropriately labeled a "confidentiality rule," it does little to put limits on the aggregation and analysis of health-related data.[142]

Health wearables, mobile apps, fitness trackers, smart watches, clothing, and similar consumer products are also outside of HIPAA's scope, except in very limited instances (such as when a device delivers patient information directly to a doctor or hospital.)[146] This gap in coverage was underscored in a July 2016 report by the Department of Health and Human Services, the federal agency responsible for implementing HIPAA regulations. The report acknowledged that a growing range of business entities, devices, and technologies that "collect, share, and use health information" are not covered by the law. These include not only "smart phones and other mobile devices," but also "peer health communities, online health management tools,

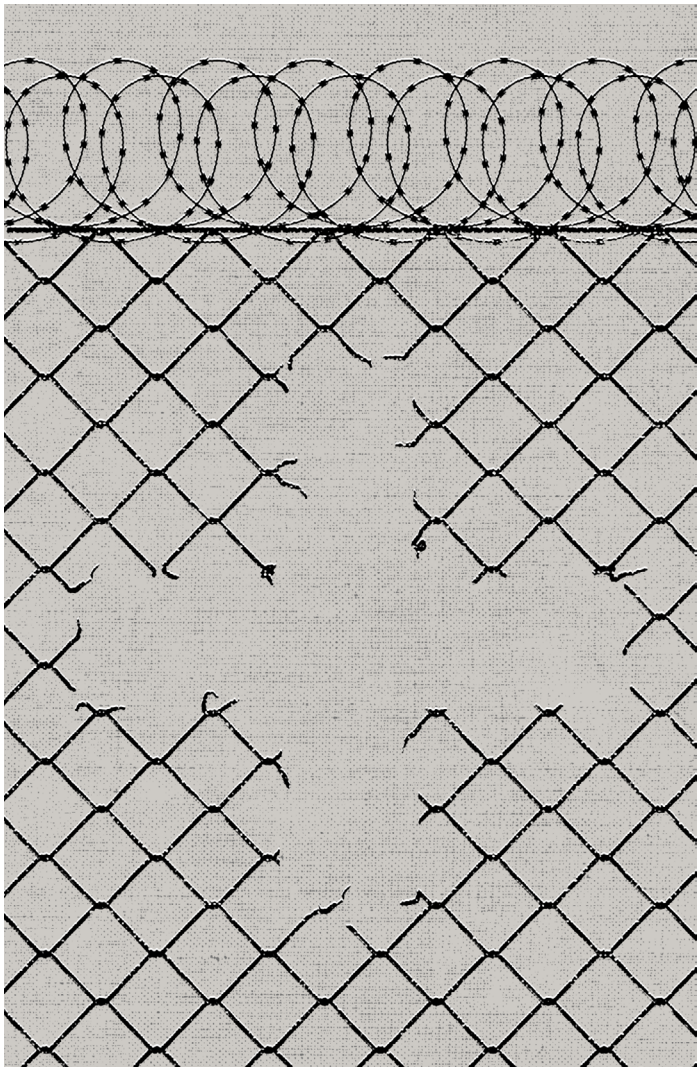
and websites used to generate information for research." Many of these "non-covered entities" (NCEs), explained the report, have "large gaps in policies around access, security, and privacy." However, while concluding that "our laws and regulations have not kept pace with these new technologies," the report fell short of making any substantive recommendations for strengthening health and medical privacy.[147]

FDA'S PRIVACY LIMITATIONS

Nor is the FDA—the federal agency that regulates pharmaceuticals, over-the-counter (OTC) drugs, and medical devices—a reliable guardian of health-wearable user privacy. While it has jurisdiction over some devices that are used to diagnose and treat diseases, it is concerned primarily with their safety, reliability, and security. The FDA recently concluded a proceeding that considered whether it should regulate health and wellness wearables. The technology industry—including prominent companies such as Samsung and trade groups like the Consumer Technology Association and Telecommunications Industry Association—strongly lobbied against such an expansion, arguing, for example, that a wearable device for tracking mood—something "similar to a 'mood ring,'" according to one filing—should be classified as a "general wellness" product along with "devices that support smoking cessation and those meant to prevent injury."[148] The FDA issued final guidance on the issue in July 2016, confirming its decision to take "a hands-off approach to the regulation of low risk general wellness products."[149] But even if it had chosen to include such devices within its jurisdiction, the agency has neither authority nor expertise to address the commercial data collection and privacy practices related to their use.

FTC'S LIMITED AUTHORITY

The Federal Trade Commission is a key government agency with responsibility to protect consumer privacy online.[150] The



GAPS AND WEAKNESSES IN HEALTH AND PRIVACY REGULATION

commission's involvement in digital privacy began in the 1990s, during the early commercialization of the Internet, amid rising public concerns over data collection. Through a series of public workshops with industry, consumer groups, academics, and other stakeholders, the agency developed its basic framework for online privacy protection, which has remained in place for the last two decades. The FTC's approach to digital privacy is based primarily on its statutory authority to regulate "unfair and deceptive" commercial practices. As a practical matter, its privacy framework has relied on a practice

known as "notice and choice." Under this system, websites, mobile operators, and other digital media companies post privacy policies informing consumers of the nature and extent of data collection.[151] The agency can take enforcement actions against companies that violate their own privacy policies or terms of service, or in other ways deceive consumers. However, the FTC lacks the statutory power to develop, implement, and enforce broad privacy rules except in very specific areas where Congress has granted it explicit authority to do so.[152] Despite its limited powers, the FTC does have a set of regulatory tools that it uses to address the rapidly expanding data-driven digital marketing system. It has conducted numerous public hearings with a variety of stakeholders, commissioned research, hired technologists, and taken enforcement action against so-called "bad actors," including some of the largest players in the digital media industry.[153] It has also served as a bully pulpit, calling attention to a wide range of problematic practices and trends.

The FTC lacks the statutory power to develop, implement, and enforce broad privacy rules except in very specific areas

In the past several years, the FTC has issued a series of reports focused on recent changes in digital marketing practices, including how companies should handle personal health information, which the agency classifies as "sensitive," along with financial data, geolocation data, Social Security numbers, and information collected from children. For example, its 2009 staff report on online behavioral advertising noted "the heightened privacy concerns raised by the collection and use of consumers' sensitive data," urging companies to obtain "affirmative express consent before collecting such data for behavioral advertising." The full

Timeline of FTC Work on Health Privacy

Jan 2011
Issues advice on medical ID theft.

May 2014
Holds workshop on "Consumer Generated and Controlled Health Data."

January 2015
Issues report on Internet of Things, urging "Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks.

April 2015
Issues tips for businesses that use consumer health data:

March 2016
Testifies in Congress on "Opportunities and Challenges in Advancing Health Information Technology."

April 2016
FTC releases new guidance for developers of mobile health apps.

May 2016
FTC continues to address heath data security via settlement of case.

June 2016
Electronic health records company settles FTC charges it deceived consumers about privacy of doctor reviews.

commission reiterated this position in its subsequent 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change."[154]

In 2014, the FTC convened academic experts, government agencies, NGOs, and industry representatives for a workshop on "Consumer Generated and Controlled Health Data" (CGHD), releasing its own in-house analysis of 12 mobile health and fitness apps, which revealed widespread dissemination of app data—including user names, real names, email addresses, medical-symptom searches, ZIP codes, geolocation, and gender—to third parties.[155] Its 2015 report on the Internet of Things, identified a number of challenges that this new generation of "smart" objects pose to consumer privacy, and offered recommendations for how companies could address them.[156] Most recently, the FTC collaborated with the FDA and HHS's Office of the National Coordinator for Health IT to release an interactive tool and legal primer for health-related mobile app developers.[157] While all of these workshops, reports, and educational materials have been useful in fostering consensus, informing stakeholders on important issues and promoting best practices, the agency can only make recommendations in the form of "guidance" to industry, which has no legal obligation to adopt them.

In those cases where it has been granted rulemaking authority by Congress, the FTC has been able to develop, implement, and enforce stronger regulations. For example, the Children's Online Privacy Protection Act (COPPA), which was enacted in 1998, requires commercial websites and other digital media that target children under 13 to limit the collection of personal information; mandates a mechanism for parental involvement; and places obligations on companies for adequate disclosure and protection of data.[158] The FTC is charged with developing regulations for implementing COPPA, investigating and fining companies that violate its provisions, and conducting periodic reviews of the regulations to ensure they remain up to date.[159] More recently, passage of the American Recovery and Reinvestment Act in 2009 granted the agency authority to conduct some limited regulation of

GAPS AND WEAKNESSES IN HEALTH AND PRIVACY REGULATION

health privacy. Its Health Breach Notification Rule sets out specific steps that vendors and "related entities" must take in the event of a data breach, including instructions for when and how to notify consumers, as well as cases in which notices to the media may also be required.[160] However, while some health wearables that meet the criteria outlined in the regulation would be subject to these requirements, the rule is narrow in scope, applying only to breaches and not to the uses of health data collected by these devices.[161]

The FTC has recently used its enforcement powers to crack down on mobile health apps that engage in deceptive practices. In February 2015, the commission negotiated two separate settlement agreements with marketers accused of deceptively claiming that their mobile apps were able to detect symptoms of melanoma, even in its early stages. The companies operating the apps—MelApp and Mole Detective—signed agreements that forbade them from continuing to make such unsupported health claims about their products.[162]

Legal scholars Daniel J. Solove and Woodrow Hartzog argue that "through a common-law-like process, the FTC's actions have developed into a rich jurisprudence that is effectively the law of the land for businesses that deal in personal information."[163] They suggest that its existing approach *could* develop into "a robust privacy regulatory regime, one that focuses on consumer expectations of privacy, extends far beyond privacy policies, and involves a full suite of substantive rules that exist independently from a company's privacy representations."[164] However, while the agency has made some progress in its ongoing efforts to address the challenges of the Big-Data era, we do not hold as optimistic a view of its current powers and potential future role. Because of its narrow jurisdiction, lack of rulemaking ability, and limited regulatory resources, the agency is ill-equipped to provide the kinds of comprehensive and granular rules that would be necessary to protect consumers, not only in the health and wearables industry, but also in the larger digital marketplace. This reality

was underscored by FTC Chairwoman Edith Ramirez's revelation of her own approach to health wearables. Speaking at the 2016 Consumer Electronics Show in Las Vegas, Ramirez acknowledged that she prefers to use a non-Internet-connected pedometer to track her exercise activity, and has refrained from getting a Fitbit because of her privacy fears over data mining of sensitive health information.[165]

The Federal Communications Commission has primary jurisdiction over broadband Internet access service companies, the phone and cable companies that supply the majority of high-speed Internet connections. In October 2016, the FCC issued privacy rules for ISPs that classify important categories of information as "sensitive," including mobile app, search engine, and health data. Before broadband network companies can gather this data for commercial purposes, they have to obtain prior consent (opt-in). This policy will not go into effect until late 2017, and it is too early to know how it will affect health privacy on the Internet.[166]

Speaking at the 2016 Consumer Electronics Show in Las Vegas, FTC Chairwoman Edith Ramirez acknowledged that she prefers to use a non-Internet-connected pedometer to track her exercise activity, and has refrained from getting a Fitbit because of her privacy fears over data mining of sensitive health information

OBSTACLES TO PRIVACY LEGISLATION

Although there has been a growing recognition that the U.S. should enact national privacy legislation to address the growth of digital data collection, none of the recent proposals has been successful. One of the latest attempts came from the White House, which in 2012 called for the enactment of privacy legislation based on a proposed Consumer Privacy Bill of Rights. The effort was aimed at providing a "comprehensive blueprint to improve consumers' privacy protections," while at the same time ensuring that "the Internet remains an engine for innovation and economic growth."[167] However, many U.S. consumer and privacy groups, viewing the proposal as inadequate, were highly critical of it.[168] Industry was also unhappy with the proposed bill, calling it "regulatory overreach."[169] Efforts to promote technical consumer-privacy solutions, such as a "Do Not Track" regime, have also failed to gain widespread industry support.[170]

GAPS AND WEAKNESSES IN HEALTH AND PRIVACY REGULATION

CHAPTER 3:

Limits of Self-Regulation

Trade groups and industry-supported nonprofits have developed a number of guidelines, codes of conduct, principles, and best practices for addressing privacy and marketing in digital media. Taken together, these various programs offer a patchwork of competing and sometimes overlapping approaches. All rely on the prevailing notice-and-choice model, claiming to give individuals control over their own personal data, and assuring them that data-collection practices are primarily intended to enhance the consumer experience in a privacy-friendly manner. However, most of the guidelines employ vague and complex language that does not accurately describe either the actual commercial operations or their impacts. Terminology such as "interest-based advertising," for example, obscures the nature and extent of data collection, analysis, and personalized targeting that these techniques actually entail. While some guidelines acknowledge that sensitive data should be better protected or respected, that concept is either poorly defined or limited to very narrow categories of information. Little is said about how consumer information may be combined with other data—including those involving finances, health concerns, race/ethnicity, and location—or how data profiles can be used to track and target consumers for advertising on various platforms.

AdChoices icon placed next to ads "more than 1 trillion times each month"[27]

"Fewer than one in 10 Internet users known what [the icon] actually means."[28]

"92% of U.S. Internet users worry about their privacy online."[29]

Researchers say that if "every Web user in the country read the policy at every site visited, time spent reading privacy policies would total an estimated 44.3 billion hours per year."[30]

52% of Americans mistakenly think the following statement is true: "When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users."[31]

If "each and every Internet user were they to read every privacy policy on every website they visit would spend 25 days out of the year just reading privacy policies."[32]

We have identified five organizations that are directly or indirectly addressing the data-collection and marketing practices involving wearables, mobile health apps, and other Internet-connected devices, as discussed below.[171]

LIMITS OF SELF-REGULATION

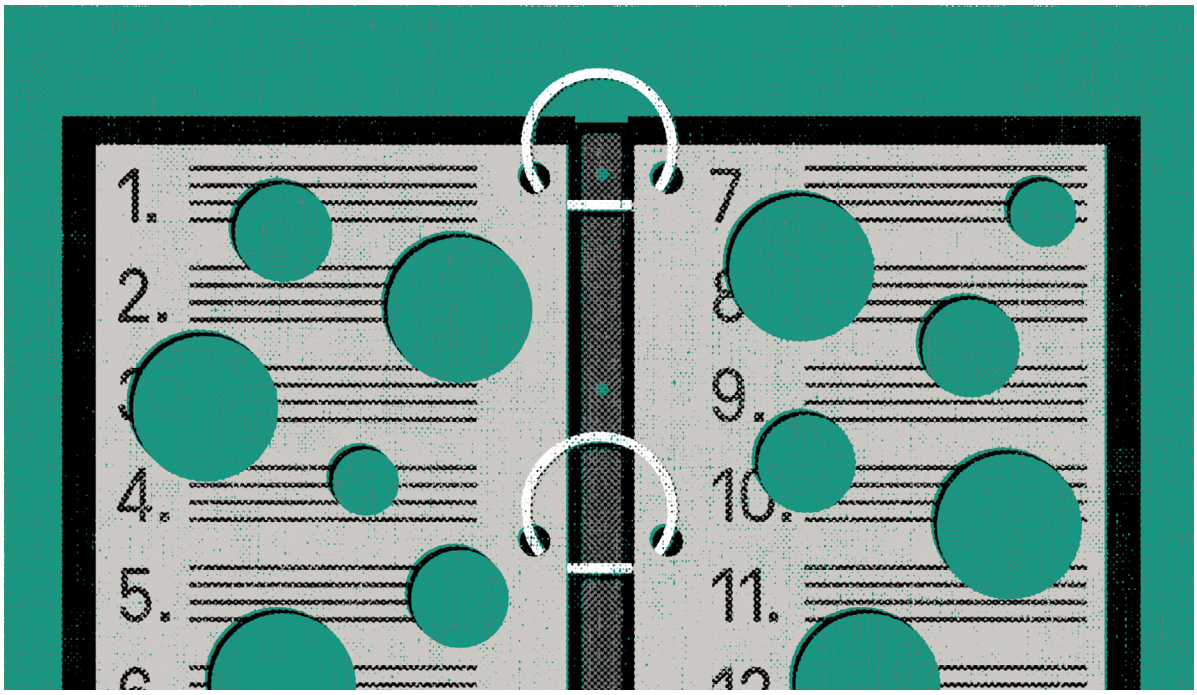
DIGITAL ADVERTISING ALLIANCE

The Digital Advertising Alliance (DAA) is considered the leading umbrella trade group administrating self-regulation of data collection and its use in online advertising. It includes the most powerful organizations in the ad industry (e.g., the American Association of Advertising Agencies, American Advertising Federation, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, and the Interactive Advertising Bureau). It has issued several recent guidance documents and tools.[172]

The DAA's main approach to protecting privacy is to require its members to adhere to its principles, and to include a "prominent" notice on each page of their online content where "interest-based" ad data are gathered. The primary form of disclosure is through an "AdChoices" tag or some other visible link, giving consumers an opportunity to "opt out" of having their online information collected for marketing purposes. The ability of consumers to make their own decisions *prior* to any data collection, known as opt-in, is available under limited circumstances, such as when sensitive data or actual geo-location is to be gathered. However, sensitive data under the DAA rules are limited to a narrow set of obvious categories, such as "financial account [and] Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual."[173] As a consequence many of the health-marketing practices that DAA member companies employ would not trigger any special requirements for handling sensitive information.[174]

NETWORK ADVERTISING INITIATIVE

The Network Advertising Initiative (NAI) represents a smaller sector of the digital marketing industry, principally those companies engaged in forms of "Interest-based Advertising" (IBA—but better known as behavioral marketing). The NAI (which is also a member of the DAA) revised its Code of Conduct in 2013 to include a variety of medically related conditions, and further updated the code in 2015.[175] It identifies as sensitive data "information about any past, present or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history, based on, obtained, or derived from pharmaceutical prescriptions or medical records, or similar health or medical sources that provide actual knowledge of a condition or treatment (the source is sensitive)." Under its framework, opt-in consent is required for so-called interest-based advertising to occur in connection with a number of health-information categories, including "all types of cancer, mental health-related conditions, and sexually transmitted diseases."[176]



But the determination of whether certain other conditions should be treated as "sensitive," according to the NAI, "can be subjective." Before gathering data and delivering ads for health marketing, NAI members are to take into consideration "the seriousness of the condition, its prevalence, whether it is something that an average person would consider to be particularly private in nature, and whether it is treated by over-the-counter or prescription medications, and whether it can be treated by modifications in lifestyle as opposed to medical intervention."[177] Under this framework, the NAI classifies high blood pressure, cholesterol management, cold, flu, and heartburn as medical conditions that do not require prior consent. The code also stipulates that "interest in diet and exercise," as well as the use of vitamins and supplements, do not trigger any prior authorization. According to the organization's health transparency requirement, consumers should be able to discover why they are being targeted by behavioral health ads when opt-in consent is not required. But the guidelines offer various options for providing this information that could allow companies to place their disclosures in very fine print.[178]

LIMITS OF SELF-REGULATION

CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association (CTA)—formerly the Consumer Electronics Association—is the trade group best known for its yearly convention in Las Vegas, showcasing the latest technology products on the market. Among its more than 2,200 members is a wide spectrum of high-tech manufacturers and digital media companies, including Google, Facebook, and Apple. Board members of its Health and Fitness Technology Division include Fitbit, AT&T, Qualcomm, Misfit, Walgreens, and Validic, among others.

CTA issued its "Guiding Principles on the Privacy and Security of Personal Wellness Data" in October 2015, including a set of voluntary "baseline recommendations" for the "health and fitness wearable ecosystem."[179] The five-page document describes "personal

wellness data" as information "that a company collects, stores, or uses about an identified user through a device, software, or service that is primarily used to collect wellness data."[180] CTA recommends that companies should "reflect broadly recognized fair information practice principles" and also have a "clear and easily understood written policy for collecting, storing, using, and transferring personal wellness data." The principles endorse an "opt-out" system for "tailored" advertising (behavioral and data-driven targeting) "based on [the] user's personal wellness data." Before personal wellness data can be transferred to "unaffiliated third parties," companies should obtain "affirmative consent."[181] However, if data have been "reasonably de-identified," the principles do not apply. The document does not suggest or require any standards for effective de-identification, leaving it entirely up to individual companies to undertake such processes, with no requirement for any explanation to their consumers.[182] Finally, the principles clearly state that they are only intended to serve as guidelines for CTA members, and that companies "will have flexibility on how to implement them according to their own unique products and offerings." There is no enforcement or oversight mechanism to ensure compliance.[183]

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a nonprofit think tank primarily supported by many of the leading digital marketing and data companies, including those involved in health-related marketing (such as Google, Facebook, IMS Health, and MaxPoint).[184] FPF has established a "consumer wellness and wearables working group" tasked with developing industry guidance.[185] Its "Best Practices for Consumer Wearables and Wellness Apps & Devices" were released in August 2016, offering what it characterizes as "a baseline of responsible practices" for the industry.[186]

The guidelines spell out a list of technical terms and definitions for determining which kinds of data are protected, and what practices companies should use in dealing with that information. However, when closely analyzed, many of the terms and practices are ambiguous and imprecise. For example, the document defines "covered data" as data collected for "non-medical lifestyle or wellness purposes," including "personal information" gathered on an individual by a "sensor-enabled device, app, or service," as well as "data that a user directly inputs."[187] But without actually stating what constitutes "non-medical lifestyle wellness purposes," the guidelines could permit collection of a wide range of information identifying a person's health or medical status. The guidelines do not define the term "personal information," nor is there mention of such technologies as "unique identifiers," which enable companies to target individuals regardless of whether they know their name or the device they use.

LIMITS OF SELF-REGULATION

The notice-and-choice model forms the basis of the FPF framework, which includes not only the use of privacy policies, but also various kinds of "enhanced notice" for soliciting "express consent" from a consumer before certain data-use applications can begin. But these processes are not entirely clear, allowing companies extremely wide latitude in how to offer and implement the provisions. For example, "covered data" can be sold to or shared with third parties by obtaining consent in several ways, including "at the point of sharing, as part of the download or installation flow," and also "via a separate process" that is not defined. The guidelines also allow marketers and app or device companies to employ these same mechanisms to get customers to opt in to collection and use of personal information related to "employment eligibility; promotion or retention; credit eligibility; healthcare treatment eligibility, insurance eligibility, underwriting, and pricing." While these requirements for "enhanced notice" and "meaningful consent" appear to provide strong safeguards, their actual implementation could result in practices that prompt consumers at any moment during their interactions with a device or app, providing easy mechanisms for giving their consent and facilitating ongoing data collection of their personal information for a variety of purposes.[188]

LIMITS OF SELF-REGULATION

Most of the industry guidelines have been carefully written in ways that do not challenge many of the prevailing (and problematic) business practices employed by their own members

The organization can be commended for taking a strong position in its "ban on sharing with data brokers, information resellers, and ad networks." However, this prohibition may not be able to address the many ways that data are shared among various players in today's Big-Data marketing ecosystem. Consumer data have become so valuable that, rather than selling that information to data brokers or ad networks, wearable companies will either be part of large digital marketing operations, or create their own ad networks and buy data themselves from marketing clouds to enhance consumer profiles in order to engage in targeted marketing.

Finally, while FPF includes directives for what companies "must" or are "required" to do, unlike membership-based self-regulatory organizations its function is only "to provide guidance" to industry, allowing significant leeway in how to interpret the recommendations.

ONLINE TRUST ALLIANCE

The Online Trust Alliance (OTA) is a non-profit association representing more than 100 companies, whose mission is "to enhance online trust and empower users, while promoting innovation and the vitality of the internet" by developing "best practices, resources and guidance to help enhance online safety, data security, privacy and brand protection."[189] OTA released its Internet of Things "Trust Framework" in December 2015, which continues to be revised.[190] The framework lays out 31 principles that should guide the development of health and fitness wearables as well as connected-home services. The framework is a "code of conduct" that primarily addresses security and privacy concerns. In contrast to most self-regulatory organizations, OTA raises serious concerns about what it describes as the "Internet of Things Time Bomb" and the "Wild West" environment in which the IoT is evolving. In accompanying materials, the OTA acknowledges that at the top of its list of "challenges" posed by the IoT ecosystem are the "highly personal, dynamic, persistent

collection and transfer of data"; the "combination of devices, apps, platforms and services"; "lack of defined standards"; and the system's multiple "data flows, touchpoints and disclosures." OTA says that "users are opening themselves up to all sorts of risks; both today and during the lifecycle of the connected device, app or service; the risk is amplified with every device connected; [there is] sharing with unknown/undisclosed parties; and it may be benign today, but harmful tomorrow."[191]

The OTA framework recommends that IoT device companies "[o]nly share consumers' personal data with third parties with consumers' affirmative consent," and that they ensure that privacy policies are "easily discoverable, clear and readily available for review prior to purchase, activation, download or enrollment." A company should also "conspicuously disclose in its privacy policy how all personally identifiable and sensitive data types and attributes are collected and used." Consumers should be provided the ability to "delete, or make anonymous personal or sensitive data stored on company servers," including if they lose, sell, or discontinue use of the device.[192] OTA has created a "voluntary code of conduct and minimum baseline requirements" for IoT products and services that will form the basis of "future certification programs" by the group. Additionally, the Obama administration has been working with industry to create a "Cybersecurity Assurance Program" to test and certify IoT devices.[193]

LACK OF MEANINGFUL ENFORCEMENT AND OVERSIGHT

While some of these current and proposed self-regulatory programs offer responsible business practices for the health wearables marketplace, their biggest weakness is that they do not provide any meaningful system of independent accountability. The mechanisms that are in place for oversight and enforcement are primarily conducted by the trade groups themselves, their partners, or individual companies.[194] Though both the major digital advertising trade groups, DAA and NAI, have programs for monitoring and enforcing their respective codes of conduct, neither appears to engage in comprehensive or systematic oversight. For example, the DAA's enforcement organization, operated by its partner, the Better Business Bureau, recently reprimanded one of these companies operating a mobile health app, requiring it to make changes in its privacy policy, including real-time notice of data collection and an opportunity for users to opt out.

LIMITS OF SELF-REGULATION

Mechanisms that are in place for oversight and enforcement are primarily conducted by the trade groups themselves

But even with the addition of these enhanced forms of notice and choice, consumers would need to know much more about how a given health app really works (including whether it uses sponsored content from health companies, for example) to be able to exercise an informed decision under the DAA process.[195]

Most of the industry guidelines have been carefully written in ways that do not challenge many of the prevailing (and problematic) business practices employed by their own members, including real-time data analysis and targeting, machine learning and predictive analytics, lookalike modeling, scoring, and loyalty programs such as e-coupons. Thus, while self-regulation may have succeeded in thwarting efforts to institute government regulations, it has failed to provide effective consumer privacy protections, and for that reason has been strongly criticized by consumer and privacy advocates.[196]

CHAPTER 4:

Developing a Public Interest Framework for Digital Health

Technology experts envision a not-too-distant future in which health and wellness devices—along with an array of next-generation Internet-connected sensors—will be fully integrated into the growing connected-health system.[197] Mobile apps and other digital tools will guide a patient through preparation and recovery from hip surgery, "analyze her daily walking patterns, provide predictive analytics on her recovery time, and engage her in physical therapy sessions."[198] These personal digital devices will not only track a person's behaviors, but also "diagnose health problems as they occur and dispatch medical care without human intervention."[199] Wearables will become part of an all-encompassing digital environment in which our personal health behaviors and bodily functions will be continuously monitored, a system made even more powerful by an automatic and instantaneous Internet of Things that utilizes a new generation of sensors embedded in the objects and tools we use every day. These devices will become a fundamental part of our everyday experiences as we continue to adapt to the now-ubiquitous presence of digital technology in our lives.

enabling people to take more control of their own health-related behaviors. "Inequality related to race, ethnicity, and socioeconomic status is one of our nation's most vexing problems," explained a report by the Department of Health and Human Services, "and it affects health status, access to health care, and health care quality." The agency is promoting public and private initiatives to connect low-income, minority, and other at-risk communities to digital technologies, which it sees as a key strategy for addressing these challenges.[200]

These new digital tools hold the promise of many health benefits, but the growth of the "wearables ecosystem" also raises a number of risks

But the growth of the "wearables ecosystem" also raises a number of risks. The flow of user-generated and biologically derived information that these devices track will be fed through a vast Big-Data network composed of hospitals, pharmaceutical companies, consumer product goods and services companies, retail stores, and many other players both within and outside the increasingly porous connected-health system. This information will be combined with millions of data points gathered from a myriad of additional sources, including public and commercial databases and data-management firms. The risks extend beyond threats to individual privacy. Algorithmic classification systems could enable profiling and discrimination—based on ethnicity, age, gender, medical condition, and other information—across a spectrum of fields, such as employment, education, insurance, finance, criminal justice, and social services, affecting not only individuals but also groups and society at large.[201] The opportunities for data breaches will increase, with hackers accessing medical and health information at insurance companies,

Without question, these new digital tools hold the promise of many benefits—empowering individuals and enhancing their health and well-being, improving the practice of medicine, and contributing more broadly to scientific research and public health. Wearable devices could also play an important role in reducing health disparities, by facilitating access to medical treatment and

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

retail chains, and other businesses. Even those institutions with the most benevolent of goals—such as public-health departments, law enforcement, and research entities—can misappropriate and misuse health data.[202] Many of the harms associated with the collection and processing of such data, moreover, are likely to affect disproportionately the most vulnerable people in our society, including the sickest, the poorest, and those with the least education.[203]

Recent surveys have already documented a growing frustration, mistrust, and cynicism among the public about the pervasive data collection in their digital lives. While the online industry argues that consumers have willingly accepted the need to give up their personal information in exchange for participation in digital culture, independent research documents that this is not the case. As a 2015 survey by the University of Pennsylvania's Annenberg School for Communication found, "Contrary to the claim that a majority of Americans consent to discounts because the commercial benefits are worth the costs, our study suggests a new explanation for what has thus far been misconstrued as 'tradeoff' behavior in the digital world: a large pool of Americans feel resigned to the inevitability of surveillance and the power of marketers to harvest their data."[204] These public sentiments are echoed in a report released by the U.S. National Telecommunications and Information Administration (NTIA), finding that "Americans are increasingly concerned about online security and privacy at a time when data breaches, cybersecurity incidents, and controversies over the privacy of online services have become more prominent. These concerns are prompting some Americans to limit their online activity."[205]

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

It is precisely because this market is in a fluid stage of innovation and growth that it is so urgent to institute clear ground rules that will guarantee that the benefits to individuals and the larger society are maximized while the risks are minimized

But it will be increasingly difficult to "opt out" of using fitness devices or mobile health apps, especially as they become further integrated into the ways we engage with medical practitioners, employers, hospitals, and other institutions. There will be incentives to use them, and many people may soon find that they cannot live without them. Even as their interactions with these digital tools become normalized and routine, however, people will not know the full nature and extent of the data collected, how they are used, and to whom that information flows. Industry plans for harnessing wearables and other connected devices for advertising purposes also raise the specter of a flood of ubiquitous, intrusive, and manipulative marketing techniques—often woven seamlessly into information and entertainment content across our digital devices and screens—that will be impossible to escape.

A WINDOW OF OPPORTUNITY

Fortunately, because this market is still being developed, we have the opportunity to build meaningful, effective, and enforceable safeguards into its foundation. Everyone in our society should be able to reap the benefits of the Big-Data era without further eroding their privacy and security, or subjecting themselves to manipulative and intrusive marketing.

Some industry organizations have argued that it is too early to develop public policies for the emerging wearables market. For example, the Future of Privacy Forum's "Practical Privacy Paradigm for Wearables" warned that "Premature regulation at an early stage in wearable technological development may freeze or warp the technology before it achieves its potential, and may not be able to account for technologies still to come."[206]

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

Key findings from the 2015 University of Pennsylvania's Annenberg School for Communication Survey:[33]

49% of American adults who use the internet believe (incorrectly) that by law a supermarket must obtain a person's permission before selling information about that person's food purchases to other companies.

69% do not know that a pharmacy does not legally need a person's permission to sell information about the over-the-counter drugs that person buys.

65% do not know that the statement "When a website has a privacy policy, it means the site will not share my information with other websites and companies without my permission" is false.

55% do not know it is legal for an online store to charge different people different prices at the same time of day.

62% do not know that price-comparison sites like Expedia or Orbitz are not legally required to include the lowest travel prices.

But we take issue with this position. It is precisely because this market is in a fluid stage of innovation and growth that it is so urgent to institute clear ground rules that will guarantee that the benefits to individuals and the larger society are maximized while the risks are minimized. Given the spectrum of unique issues and concerns raised by these devices, privacy, security, and consumer-protection policies for the health-wearables market should be held to a much higher standard than that established for most other areas of the digital marketplace. Addressing these concerns requires a comprehensive framework that will ensure true accountability and enable effective enforcement. Many people in the consumer, privacy, professional, and academic communities have highlighted the need for industry and government alike to develop new approaches to the protection of personal health information in the Big-Data era.[207] If effective policies can be put in place now, consumers will have legitimate reasons to trust the companies with which they do business, and will gain confidence in the fairness of the overall consumer marketplace. Rather than stifling innovation, these policies will both foster and guide the growth of the industry.

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

KEY PRIVACY PRINCIPLES

Although the focus of this project is primarily on policies for the consumer wearables marketplace, it is increasingly difficult to separate these products and services from the broader connected-health system. The digital environment and our online lifestyles have created a highly permeable system in which traditional concepts of medical, health, and wellness information are now much less distinct.[208] Because regulation is so fragmented and insufficient, we see an urgent need for a much broader policy framework to protect health privacy. Nor is it possible to address the health and fitness wearables market without considering the need for a more expansive approach to digital and online media in general. Thus our approach is to identify the key principles and critical issues that need to be considered in developing effective privacy and consumer protections for the emerging digital health marketplace.

PRIVACY AS A FUNDAMENTAL RIGHT

We begin by underscoring a first principle that too often gets lost in the complicated and technical inside-the-beltway policy discourse: that privacy is not just a preference, but rather a fundamental and inalienable right. Privacy has a long and established legacy, both internationally and in the U.S., and is firmly embedded in many of our basic legal institutions. Moreover, privacy is essential to such core democratic values as autonomy, self-determination, and dignity.[209] It is important

not to lose sight of this right. There will likely be instances when people will want to—or need to—share information about themselves through wearable devices, Internet-connected tools, and other digital platforms. But the consumer interfaces and internal algorithms of these services should not treat the right to privacy as merely optional or negotiable, especially in commercial environments where individuals face powerful corporations and institutions that can set the terms and conditions for entry or participation, often with all-or-nothing choices, unclear agreements, multi-layered caveats, and incentives designed to influence consumer decision making. The tradeoff for reaping the benefits to our health-care system made possible by digital devices should not be surrendering control over our personal data.

TWENTY-FIRST-CENTURY BIG-DATA SAFEGUARDS

For decades, privacy and data-protection policies—in both Europe and the U.S., as well as in many other countries—have been guided by Fair Information Practices, sometimes called Fair Information Practice Principles (FIPPs).[210] FIPPs are considered the gold standard of privacy policy, a framework that combines a set of rights for individuals with a clear articulation of responsibilities to govern how institutions can collect and use personal data.[211] The FIPPs framework of eight principles was codified in the 1980 "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," reaffirmed in 2013 and embodied in laws and regulations throughout the world.[212] (See sidebar: "The OECD Privacy Principles.") While several versions of the principles have evolved over the years, both globally and in the U.S., their core elements have remained in place.[213] Most recently, both the FTC and the Obama White House have proposed new policy frameworks that are based on FIPPs.[214]

In both theory and practice, the Big-Data paradigm contradicts and undermines some of the basic principles embodied in FIPPs.[215] For example, the principle of *data minimization* means that there should be limits on the kinds and amounts of information an organization, government, or company can collect from an individual.[216] Closely allied to this notion are the related principles of *data quality, purpose specification,* and *use limitation,* which stipulate that personal data collected from individuals should be accurate and used only in ways that are consistent with the reason for collecting that information in the first place. But practices at the heart of Big-Data systems are in direct opposition to these important principles, relying on *maximizing* data collection and *repurposing* information for ongoing, secondary, and even unforeseen uses. As Viktor Mayer-Schönberger and Kenneth Cukier explain in their influential book, *Big Data: A Revolution that Will Transform How We Live, Work, and Think,* "datafication" involves "taking information about all things under the sun—including ones we never used to think of as information at all…and transforming it into a data format to make it quantified" in order to unlock its implicit, latent value.[217] "Ultimately, the value of data is what one can gain from all the possible ways it can be employed.... In the big-data age, data is like a magical diamond mine that keeps on giving long after its principle value has been tapped."[218]

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

The tradeoff for reaping the benefits to our health-care system made possible by digital devices should not be surrendering control over our personal data

Another fundamental tenet of the FIPPS framework is that users should have control over their own personal data, which is articulated in a set of *user participation* rights; these include the ability to find out what data have been collected about them, and to challenge or correct that information.[219] But Big-Data operations such as machine-learning

CONTINUED ON PAGE 55 →

OCED Privacy Principles[34]

1. **COLLECTION LIMITATION PRINCIPLE**

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **DATA QUALITY PRINCIPLE**

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. **PURPOSE SPECIFICATION PRINCIPLE**

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **USE LIMITATION PRINCIPLE**

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [the Purpose Specification Principle, above] except:

a. with the consent of the data subject; or

b. by the authority of law.

5. **SECURITY SAFEGUARDS PRINCIPLE**

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. **OPENNESS PRINCIPLE**

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **INDIVIDUAL PARTICIPATION PRINCIPLE**

An individual should have the right:

a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b. to have communicated to him, data relating to him

i. within a reasonable time;

ii. at a charge, if any, that is not excessive;

iii. in a reasonable manner; and

iv. in a form that is readily intelligible to him;

c. to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. **ACCOUNTABILITY PRINCIPLE**

A data controller should be accountable for complying with measures which give effect to the principles stated above.

algorithms, artificial intelligence, predictive modeling, and fully automated programmatic ad campaigns make it increasingly difficult for people even to know what information is collected about them, and to understand how that information is used, let alone have any control over it. With digital tools and platforms seamlessly interwoven into our daily activities, and as Big-Data practices become more complex and opaque, consumers are now at a decided disadvantage in trying to make sense of their privacy options—if, in fact, such options actually exist.

This underlying conflict between traditional privacy principles and Big-Data imperatives has prompted some to declare that FIPPs are simply no longer relevant.[220] But rather than abandoning FIPPs, we need to strengthen and supplement these long-standing principles, exploring ways to correct many of the problems associated with their application in U.S. privacy policy to date, and assessing how they can be augmented in the era of Big Data. We also need to build on this framework by developing additional standards and practices that can address a host of new and emerging data operations. This 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.[221]

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

Big-Data operations such as machine-learning algorithms, artificial intelligence, predictive modeling, and fully automated programmatic ad campaigns make it increasingly difficult for people even to know what information is collected about them

BEYOND "PRIVACY SELF-MANAGEMENT"

The prevailing model of *notice and choice*—which has been embraced by both government regulators and industry—operates on the assumption that an individual will review the disclosures in a company's privacy policy, evaluate the pros and cons for herself, and, if she uses or purchases the product or service, will agree to the terms of the data-processing arrangement.[222] However, a growing body of research by privacy scholars and data-protection experts has determined that such traditional privacy mechanisms—even when using an "opt-in" model, and updated and adapted as "just-in-time" notices or mobile app consent tools—are increasingly inadequate in today's Big-Data digital marketplace.[223] Far too often such policies, written by lawyers in purposefully obtuse and arcane language, simply fail to make clear to users how their data are collected and used.[224] As with other "terms-of-service" statements, most privacy policies offer no real choice; instead, they are presented as "take-it-or-leave-it" propositions.[225]

While the FTC has suggested a number of ideas for adapting the notice-and-choice model for the wearables and Internet of Things era—"developing video tutorials, affixing QR codes on devices, and providing choices at point of sale, within set-up wizards, or in a privacy dashboard"—it is questionable whether these techniques would be effective.[226] Even if disclosures could be simplified, in today's hyper-connected world there are so many occasions for individuals to provide consent that it is practically impossible for anyone to handle the deluge of decision points.[227]

Such expectations of "privacy self-management" are at odds with contemporary Big-Data practices.[228] Legal scholar Frank Pasquale cautions against viewing consumer "control" as a "be-all, end-all solution to health privacy matters." Although he is writing mainly about patient privacy in the medical context, his point applies equally to

all aspects of the connected-health and digital wearables marketplace, where it is virtually impossible for individuals to manage the complexities of data collection and use of their own health information. As Pasquale explains, many patients "either can't be responsible (or don't want to be responsible) for exercising control over health data. Paradoxically, the sickest, most vulnerable persons may be the ones with the most data to manage—and the least time or energy to take on this oft-neoliberal concept of identity management." Therefore, "any aggressive promotion of the Control Solution must be complemented with ongoing, equally aggressive efforts to outlaw or otherwise reduce problematic uses of health data," he explains.[229]

IMPROVING TRANSPARENCY

Our assessment of the flaws in the current notice-and-consent system does not mean to suggest that companies should abandon their responsibility to make their data collection and marketing practices transparent to consumers. Meaningful and effective transparency is consistent with the FIPPs principle of *openness.*[230] However, based on our own analysis of the privacy policies posted by several leading companies in the wearables market, current disclosure practices fail to explain the full spectrum of data collection, sharing, and marketing techniques employed on these devices, leaving a great deal of room for improvement.[231] A few companies appear to offer stronger safeguards than others. We note, for example, that Apple's strong approach to consumer privacy sets it apart from most of the other players in the market. Its privacy policy promises that a user's data will be kept on her mobile phone, Apple Watch, or other device, making it impossible for outsiders to access the information. However, overall the privacy policies in this sector display many of the same kinds of problems that scholars have documented in other parts of the digital media marketplace.[232] (See Appendix B, "Analysis of Wearable Privacy Policies.") According to Professor Joseph

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

Turow, many privacy policies purposely frame their practices in a manner designed to placate consumers, using language that affirms the company's promise to protect consumer privacy, for example, while peppering the policy with jargon that consumers cannot understand and "misnaming" certain procedures, "tagging an activity in a way that leads people to consider it less problematic than it actually may be."[233]

Transparency needs to go beyond corporate privacy policies and terms of service. The pervasive use of algorithms in many sectors of our society—including social media, marketing, science, and government—has triggered rising concern about how these

Based on our own analysis of the privacy policies posted by leading companies in the wearables market, current disclosure practices fail to explain the full spectrum of data collection, sharing, and marketing techniques employed on devices

"black box" operations can negatively impact individuals, communities, and groups.[234] To address this problem, leading public interest organizations and scholars are calling for "algorithmic transparency."[235]

REDEFINING "PROTECTED DATA"

Both regulatory agencies and industry self-regulatory organizations classify certain kinds of information as "sensitive," and thus deserving of greater privacy protection.[236] While personal health information should clearly be considered sensitive, it is important to understand that in the Big-Data era, no single piece of data or category

of information can easily be isolated for special handling. We need to think of the system more holistically, as the aggregation of many "data points" about an individual, across multiple platforms and digital devices, online and off, that reveals important and "actionable" insights about a person's health.[237] Companies that operate health devices and apps gather a great deal of personal information about consumers that extends far beyond a set of narrowly defined, specific health or wellness data points. This can include one's race, ethnicity, gender, income, or sexual orientation, as well as continuous tracking of an individual's spending activities, geolocation movements, and social interactions. Device companies can obtain further information about their customers from data brokers and other sources. As a consequence, these new health and wellness tools can create rich and highly valuable personal health profiles that marry daily monitoring of biometric functions, physical activity, and other health data with a spectrum of additional information about an individual's attributes and behaviors. So, for example, a device or mobile app that tracks physical activity would be able to know many things about the consumer who uses it, such as that fact that she is a diabetic Hispanic woman living in a poor part of the city, that she shops at Walmart for her food, that she frequently buys high-calorie chips, cookies, and other unhealthy foods, and that her exercise patterns are inconsistent and erratic.

Restricted categories of so-called personally identifiable information (PII) are equally problematic and outmoded in today's digital marketing environment. Virtually all of the wearable company privacy policies we examined offered assurances to users that their PII was protected, with statements such as this one, in Under Armour's policy, referring to its practice of collecting only "information that is anonymous, aggregate, de-identified, or otherwise does not reveal your identity."[238] But commonly employed Big-Data techniques have rendered such definitions meaningless, creating a myriad of ways to identify and target individuals without ever needing the person's name, email address,

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

or other traditional identifying information.[239] De-identification and anonymization, though endorsed by regulators, are only partial solutions.[240] As Barocas and Nissenbaum make clear, "even where strong guarantees of anonymity can be achieved, common applications of big data undermine the values that anonymity traditionally had protected. In cases where people may not technically be considered 'identifiable,' they are still 'reachable.'"[241]

LIMITING COLLECTION AND REGULATING USE

When purchasing a fitness tracker or other health wearable device, users should not face a situation where companies have *carte blanche* to collect as much information as they want.[242] The principle of "respect for context" has been articulated by scholars and endorsed by the Obama White House in its Consumer Bill of Rights, which affirms that "consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent

The pervasive use of algorithms in many sectors of our society—has triggered rising concern about how these "black box" operations can negatively impact individuals, communities, and groups

with the context in which consumers provide the data."[243] Some of the industry self-regulatory codes have incorporated language about "context" and "consumer expectations" into their guidance to companies.[244] But the vague language gives too much control to corporations for choosing how to interpret such guidance. And while these codes may include worthwhile ethical

"best practices," they are contrary to business models that are built around maximizing and monetizing consumer health data. Given the choice between ethics and economics, companies cannot necessarily be expected to exercise restraint.

Restricting the data collected through the device itself (so-called "first-party data") solves only part of the problem, especially since companies routinely combine that data with a spectrum of additional information about individuals that comes from outside companies, databases, and data-management firms (i.e., third-party data). In order to ensure meaningful privacy for personal health information, we need to think about how to address the data flow among these various partners—and their intended and potential uses. If we are to expect a consumer to "opt in," there must be widespread understanding of what the consequences will actually be. Wearables and other health-tracking devices offer new opportunities for individuals to share their health and medical data, reaping the many benefits of large data analysis and access to health information. But users should be able to make data-sharing decisions in a context of genuine trust and safety.

Policy makers should consider establishing more effective ways to assess both the benefits and risks of data use—not only to individuals, but also to groups and the larger society. Data-technology practices should be required to undergo some form of risk-impact assessment before they are put in place.[245] While industry self-regulatory organizations can play a role in this process of risk-impact assessment, risk/benefit analysis, and the establishment of acceptable data-use categories and risk levels, they should not be the sole arbiters of decision making in any of these areas.[246] To ensure adequate transparency, accountability, and enforceability, all of these processes should be conducted by third-party entities, with the involvement of independent consumer and privacy organizations, and under the supervision of regulators. The results of these analyses should be made available to the public, including the creation of accessible, consumer-friendly materials comparable to nutrition labels, illuminating how certain uses of personal health data, while offering a number of benefits, might also create additional risks to individuals or groups.

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

Policy makers should consider establishing more effective ways to assess both the benefits and risks of data use—not only to individuals, but also to groups and the larger society

NEW REGULATORY STRUCTURES AND APPROACHES

The current regulatory system for the health and wearables marketplace is both weak and fragmented, with jurisdiction split among several different federal agencies, each lacking sufficient authority or regulatory tools to establish and implement meaningful consumer safeguards. As we consider how best to approach privacy, consumer protection, and other Big-Data issues, it is useful to look at regulatory structures in other industries whose operations are complex and where certain practices pose a variety of risks. We have passed laws to establish agencies and independent third parties that have the knowledge and expertise to evaluate the efficacy and safety of drugs, cars, and industrial practices affecting the environment. Businesses operating within these industries are required to build these "externalities" into their operations, creating a level playing field both within the industries themselves and for consumers who interact with them. For example, in areas such as banking, auto manufacturing, and food production, we have established a system of safeguards for consumers, best practices for companies, and government agencies that can ensure those safeguards will actually work. In all of these sectors, consumers may have many choices, but there are a variety of systems in place to ensure they are not forced to understand the complex operations of all the products and services in order to manage their own risks. So, for example, we now have regulations to ensure that banks do not engage in predatory lending; that food processing plants' output is safe from disease, toxins, and other harmful elements; and that cars are equipped with safety features that protect drivers and their passengers alike. The dangers of Big-Data practices may seem less dramatic than the more obvious harms of unsafe autos or food, but they are equally important, and their implications just as serious.

Exactly what a new regulatory structure should include will require broad discussion among the major stakeholders involved. But

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

a number of possible options should be considered. One possibility would be for Congress to grant the Federal Trade Commission specific authority to regulate health privacy in the consumer arena. This was the model for the 1998 Children's Online Privacy Protection Act. While that statute was narrowly defined to focus only on protections for children under 13, it expanded the FTC's regulatory authority by mandating that the agency develop new rules to enforce and carry out the terms of the law.[247] Such a law for health privacy would enable the FTC to conduct rulemaking procedures, develop regulations, monitor industry compliance, and take enforcement actions. Another option would be to establish a separate, independent government agency for health privacy regulation.[248]

Safeguards are needed so that personal health information is not used for marketing purposes that are unfair, deceptive, manipulative, or discriminatory

The rise of Big Data and its extensive and varied impacts may necessitate the creation of a new government entity with an even wider mandate. Privacy advocates have been arguing for years for the establishment of a data-protection authority to replace our current structure of privacy regulation in the U.S.[249] Given the widespread and transformative nature of data-driven operations and practices across multiple sectors of our society, a holistic regulatory structure would be better able to manage a broad spectrum of issues, ensuring ethical data-processing practices, instituting effective consumer privacy safeguards, and preventing discriminatory uses of data.[250] While some of these ideas may seem unrealistic in the current political environment, we believe it is important not to narrow or reduce our expectations, especially

CONTINUED ON PAGE 61 →

Culture of Health Vision: Underlying Principles[35]

1. Good health flourishes across geographic, demographic, and social sectors.
2. Attaining the best health possible is valued by our entire society.
3. Individuals and families have the means and the opportunity to make choices that lead to the healthiest lives possible.
4. Business, government, individuals, and organizations work together to build healthy communities and lifestyles.
5. Everyone has access to affordable, quality health care because it is essential to maintain, or reclaim, health.
6. No one is excluded.
7. Health care is efficient and equitable.
8. The economy is less burdened by excessive and unwarranted health care spending.
9. Keeping everyone as healthy as possible guides public and private decision-making.
10. Americans understand that we are all in this together.wearable devices, or any other digital enterprise, are under no such legal or ethical constraints.

at a time when we still have an opportunity to help influence how Big-Data operations and practices evolve.

Regulating digital pharmaceutical and health marketing. As this report has documented, the business models and commercial imperatives that are shaping not only the consumer wearables industry, but also the entire media system, are based on the monetization of consumer data in order to deliver targeted advertising to specific individuals.

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

Exactly what a new regulatory structure should include will require broad discussion among the major stakeholders involved

The marketing and advertising techniques emerging in the health and wearables arena call for an ethical and policy agenda that will ensure fair practices. Safeguards are needed so that personal health information is not used for marketing purposes that are unfair, deceptive, manipulative, or discriminatory. The practices documented in this report include a range of techniques that need to be investigated, such as condition targeting, programmatic marketing, scoring, and lookalike modeling, along with a range of location-based targeting applications as well as in-store and digital outdoor marketing. Many of these practices operate under the radar of consumer knowledge or perception, making them difficult to discern or resist.

Direct-to-consumer pharmaceutical marketing has already raised many concerns among health professionals, consumer organizations, and public-health groups.[251] The American Medical Association (AMA) recently passed a resolution calling for a ban on DTC advertising, because of concerns that this form of prescription-drug marketing interferes with the doctor-patient relationship and drives up the cost of medicine.[252] Digital media, mobile, and wearable technologies have ushered in an entirely new generation of DTC pharmaceutical marketing, taking advantage of rich consumer data and profiles harvested from numerous sources to target individuals with personalized messages. Drug companies are now able to acquire and process increasingly granular information about individuals, related to their personal health behaviors, illnesses and ailments, use of medical facilities, retail shopping patterns, and even daily mood shifts and psychological states of mind. Policy makers should investigate how these new practices may be compounding the existing problems of DTC marketing.

Lobbyists for the pharmaceutical industry often argue that advertising is necessary in order to educate patients about their medical options, and to empower them to make their own decisions without having to defer solely to health professionals. While patient empowerment is important, and now much easier in the digital age, advertising is not necessarily a fair, neutral, or accurate way to empower people. Research on DTC pharmaceutical TV commercials, for example, has shown that the required "small-print" notices with warnings of side effects—even with a voiceover reading them—are often ignored or not understood because of the clever juxtaposition of powerful images and music that sends the opposite message.[253] Digital versions of DTC marketing are more personalized and less transparent, employing an array of data-driven profiling and targeting techniques that may serve to undermine consumers' ability to make rational decisions rather than informing them of their options.

Policy makers need to assess the adequacy of current advertising regulations in addressing the Big-Data marketing techniques not only of pharmaceutical companies, but also of a range of players in the health and medical industry. Today's digital practices have outpaced federal safeguards, calling for much more proactive research on contemporary market trends and closer scrutiny of emerging practices.

Protecting the patient-consumer across the connected-health landscape. In its recently released "roadmap," the HHS Office of the National Coordinator of Health Information Technology (ONC) called for action to "move beyond EHRs (electronic health records) as the sole data source for electronic health information to a wider range of health information technologies used by individuals, providers and researchers." The plan envisions that over the course of a transitional period between 2021 and 2024, individuals will gradually gain control over their health information "across online tools [and] mobile platforms and devices." A key principle for implementing this vision is to "protect privacy and security in all aspects of interoperability and respect individual preferences."[254] (See Appendix C, "Recent Federal Privacy Initiatives.") We believe it is important to build on this national priority roadmap. However, it will not be possible to develop safeguards or empower individuals across the connected-health system until we fully understand the complex web of data brokers, data-management systems, hospitals, pharmaceutical companies, medical marketing companies, and others involved with medical and health data.

Safeguards for commercial-academic research partnerships. Many of the companies in the consumer-wearables market have already forged partnerships with prominent universities and other research institutions to conduct a variety of studies that rely on consumer-wearable devices for collection and analysis of health research data.[255] This is a trend that promises to transform the practice of scientific and medical research, enabling large-scale studies to be conducted at a fraction of the cost required for more traditional controlled experiments, and giving researchers enhanced opportunities to take advantage of the many benefits of Big Data to generate valuable results.[256] But such ventures are also blurring the lines separating the commercial, government, and nonprofit arenas. A number of government and private initiatives are currently underway to develop ethical and privacy frameworks for Big Data, including procedures for how wearable devices, mobile apps, and similar technologies can be used in research projects.[257] If carried out effectively, such programs could help ensure that research institutions with a strong tradition of ethical practices will have protocols to enable them to conduct their research responsibly in the Big-Data era. But it remains unclear whether rigorous regulations in the public and academic sectors will significantly influence the standards and practices in the private, commercial sector. Companies whose business model involves the monetization of consumer data have a conflict of interest when partnering with research institutions, and as a result those research institutions need to redouble their efforts to ensure privacy protections for data subjects in their studies. The relationships between research institutions and the companies with which they collaborate will need to be spelled out very clearly to ensure adequate safeguards for patients and consumers. (See sidebar: "Developing Research Protocols for Wearables.")

DEVELOPING A PUBLIC INTEREST FRAMEWORK FOR DIGITAL HEALTH

Ensuring fairness and equity in health technology. Communities of color have long been subjected to disproportionate degrees of government surveillance and commercial mistreatment. As efforts are undertaken to promote these technologies and services to underserved communities, we will need to ensure that public policies and industry practices are put in place to guarantee fair and equitable treatment. The hidden algorithms, data-management systems, and profiling operations that are a central part of the Big-Data engine should not be allowed to foster processes that discriminate according to race, gender, medical condition, or socioeconomic status.[258] A growing movement is underway among civil rights organizations and others to prevent the growth of a new generation of discriminatory practices.[259] We also need to ensure that programs for providing access to health technology for low-income groups do not require people to give up their data in exchange for discounts to products and services. Such "pay-for-privacy" practices could create a new "privacy divide," mirroring the digital divide that has attracted widespread attention since the 1990s.[260]

Developing Research Protocols for Wearables

Scientific research at universities or federally funded institutions is subject to a rigorous set of protocols designed to ensure that individuals involved in the studies are not treated unfairly or harmed in any way, and that they are involved in the research only if they give their prior informed consent to participate.[36] For example, if a university researcher wants to conduct interviews, experiments, or any other type of study involving human participants, she is required to comply with a complex set of rules, administered by the university's Institutional Review Board (IRB) to ensure that the design and implementation of the study follows strict ethical procedures. Private companies, however, including those involved with mobile apps, wearable devices, or any other digital enterprise, are under no such legal or ethical constraints.

The absence of protections within the commercial sector has already raised concerns among public health professionals, academics, and potential research subjects. For example, a study by a team of researchers at the University of California, San Diego, explored the barriers to using personal health data (PHD) in research generated by personal fitness and wellness trackers, finding that "[a]mong individuals surveyed, the dominant condition (57%) for making their PHD available for research was an assurance of privacy for their data, and over 90% of respondents said that it was important that the data be anonymous. Further, while some didn't care who owned the data they generate, a clear majority wanted to own or at least share ownership of the data with the company that collected it." But the report also noted that no existing government regulations protect user privacy in this area, nor is it possible to anonymize user information successfully, or prevent the re-use of data.[37]

The Robert Wood Johnson Foundation's Data for Health Initiative identified similar concerns in the course of a "listening tour" that it conducted in five cities around the country. While many groups and individuals, particularly those focused on overcoming diseases, were eager to share health data that could advance research and improve health care, they were also worried about safety, privacy, and confidentiality. Among the report's recommendations was the need to "[s]trengthen the right of individuals to access and obtain their health data." As the report explained,

> Frequently, individuals are treated as second-class citizens when they try to exercise these rights. Policies should establish clear, equal rights of an individual to obtain data about his or her health—akin to a Bill of Rights. Policies should empower individuals and enable them to make decisions about their own health and contribute to decisions that can improve

Developing Research Protocols for Wearables

> the health of their communities.... The United States needs a set of laws, policies and procedures governing devices that generate personal health information.[38]

In November 2015, the White House released its "Privacy and Trust Principles." Covering six distinct areas—governance; transparency; participant empowerment; respect for participant preferences; data sharing, access, and use; and data quality and integrity—the "principles articulate a set of core values and responsible strategies for sustaining public trust and maximizing the benefits of precision medicine."[39] Within the university sector, a research team at the University of California, San Diego, has received funding from the Robert Wood Johnson Foundation to launch the Connected and Open Research Ethics (CORE) project, whose goal is to create a "web-based resource that will help scientists and Institutional Review Boards (IRBs) design and conduct ethically sound research involving personal health data collected from sensors, social media and mobile devices."[40] Sage Bionetworks has created a Participant-Centered Consent (PCC) toolkit for electronic informed consent, or e-consent. The toolkit is aimed at people who are designing clinical studies and who wish to make their informed-consent process "user-centered, rather than document-centered. It contains the building blocks of a visual, interactive approach to informed consent. The PCC toolkit lets its users create visual summaries of consent forms, mapped to key underlying text, for use in software or print." The toolkit is in use by five active studies, and "currently supports minimal-risk studies that collect sensor data, survey data, and data collected via the Apple Health application."[41]

Apple's ResearchKit could serve as a model for ensuring that protocols for protecting human subjects in scientific research are extended to partnering commercial platforms. ResearchKit is a set of open-source developer tools that are designed to enable researchers to develop and conduct clinical studies through iPhone apps. Individuals can choose the studies in which they are willing to participate, and the ResearchKit software will select the specific kinds of data needed for the study.[42] Apple has already partnered with a number of hospitals and medical research institutions for a variety of projects. For example, Johns Hopkins has developed an app for the Apple Watch that also allows consumers to opt in to participation in a research study. According to the Hopkins website for this application, "EpiWatch gives you a chance to help epilepsy research by sharing the data about your seizures. By entering data into EpiWatch, you can monitor your condition as you help Johns Hopkins researchers better understand epilepsy and potentially improve treatment."[43] Individuals who want to participate in the study must download an application that explains what will happen with their medical data and then sign a consent form, similar to what they would sign if they were involved in any other clinical study. The information in the privacy statement promises it "will not sell, rent, or lease, your Personal Information" gathered through the app. It also explains that "JHU or its third-party provider may gather general anonymous behavior data about you to help JHU or its third-party provider to better understand patient population make-up and how to improve outreach to potential sub-groups of patients under-represented in the study. JHU will not sell such data. JHU will not use such data to create or deliver

Developing Research Protocols for Wearables

ads. JHU will use such data to understand and improve clinical trial recruitment."[44] For users, the app "helps you manage your epilepsy by tracking your seizures and possible triggers, medications and side effects. You can view this information at any time, and a dashboard lets you share a summary of the data with your doctor or caregiver if you want. With EpiWatch, you can also send a message to family members or caregivers to let them know when you are tracking a seizure. EpiWatch gives you a chance to help epilepsy research by sharing the data about your seizures."[45]

Apple's ResearchKit policy is consistent with the company's overall approach to privacy in all of its products and platforms. The privacy policy adopted by Apple reflects the larger goal of providing users with greater control of their own data.[46]

Other commercial players in the wearables market may not offer as many protections when partnering with research institutions.

We recommend that there be a universally agreed-upon system that is flexible enough to enable innovations in research, but clear and strong enough to ensure that patient privacy is protected and risk is minimized. Such rules should be universal—applying to all entities and protocols, and covering corporate alliances with research, medical, and health institutions.

From an institutional perspective, one especially promising idea has been put forward by John Wilbanks and Marty Tenenbaum involving the creation of a health research commons. Similar in some respects to the Morrill Land Grant College Act of 1862 (in which the proceeds from the sale of public lands in the West were used to fund state colleges and universities), a digital health commons would serve as "a virtual marketplace or ecosystem where participants share data, knowledge, materials and services to accelerate research....

> Individual researchers, institutions, and companies will be able to publish information about their expertise and resources so that others in the community can readily discover and use them. Core competencies, from clinical trial design to molecular profiling, will be packaged as turnkey services and made available over the Net. The Commons will serve as the public-domain, non-profit hub, with third-parties providing value added services that facilitate information access, communication, and collaboration.... The Health Commons is too complex for any one organization or company to create. It requires a coalition of partners across the spectrum. It is also too complex for public, private, or non-profit organizations alone—reinventing therapy development for the networked world requires, from the beginning, a commitment to public-private partnership. Only through a public-private partnership can the key infrastructure of the Commons be created: the investments in the public domain of information and materials will only be realized if that public domain is served by a private set of systems integrators and materials, tools and service providers motivated by profit. And in turn, the long-term success of the private sector depends on a growing, robust, and self-replenishing public domain of data, research tools, and open source software.[47]

CHAPTER 5:

Empowering Consumers, Protecting Privacy, and Ensuring Equity in the Connected-Health Era: Best Practices and Next Steps

Establishing effective safeguards for the wearables and connected-health marketplace will require widespread participation across many sectors of our society, including the high-tech and health industries, academic institutions, nonprofits, foundations, policy makers, and communities. In this chapter we offer several suggestions for next steps toward that goal, including some specific recommendations for industry.

BEST PRACTICES AND NEXT STEPS

Strengthening public interest and nonprofit participation

Consumer, privacy, civil liberties, and civil rights groups should play a more proactive and collaborative role in the policy process. We propose the creation of a Public Interest Connected-health Task Force, supported by foundations, to bring together the expertise of a wide spectrum of organizations committed to privacy, consumer protection, and equity in the Big-Data era, including those groups committed to the goal of "data justice."[261] Such an initiative would require sufficient resources to enable the entity to undertake a number of important tasks, including analyzing new developments, developing public policy and self-regulatory proposals, conducting outreach to other key stakeholders, and engaging in constructive dialogue with industry and government officials. This task force could also help ensure that nonprofits are better represented on government advisory boards, multi-stakeholder initiatives, and rulemaking proceedings at federal agencies.

Promoting public education

Consumer and civil rights organizations should be encouraged to inform their constituencies and the public at large about the issues raised by the role of digital technologies in the connected-health marketplace. The conversation needs to be taken outside of the DC beltway, engaging people at the state and local levels in discussions that broaden the debate beyond its narrow technical and policy focus. For example, the benefits of Big Data are often framed around efficiency, freedom, innovation, competitiveness, and profitability. While these are important goals, they sometimes overshadow consideration of other equally important values—such as equality, fairness, diversity, community, and dignity—that must also be addressed as we assess the benefits and risks of Big Data's impact on the connected-health system.

Developing a collaborative and cross-cutting research agenda

As the forces of Big Data and digital technology continue to transform the health system, ongoing research will be necessary in order to inform policy makers, health professionals, and the public. Representatives from academic institutions, civil society, and philanthropy should work together to develop a comprehensive, interdisciplinary research agenda drawing from the expertise in a wide spectrum of fields. For example, studies should be commissioned to map, analyze, and assess data operations and business operations across the connected-health landscape, and to evaluate the costs and benefits of such practices, including their potential consequences for particular communities and populations.

BEST PRACTICES AND NEXT STEPS

Fostering stronger industry best practices

We encourage individual companies involved in the health and wearables market to make their privacy and consumer-protection commitments public, and to explain how they intend to carry them out, as part of their annual corporate responsibility and shareholder reports. We also urge industry-wide trade organizations to work with privacy, consumer, civil liberties, and civil rights organizations to develop best practices, which would help to establish a level playing field for both wearables companies and their consumers. An urgent task for such an initiative would be to address the challenges that contemporary data processes pose to meaningful consumer decision making. While the exact provisions would need to be further developed, we offer the following set of principles. They are designed to give consumers as much control over their own data as possible, while establishing default safeguards for both the collection and use of that data.

- **Sensitive Information:** *All* data collected from a health or wellness wearable device should be considered sensitive, and thus require an affirmative and effective consent process. Consent mechanisms should go beyond the notice-and-choice model, offering individuals straightforward, user-friendly, and granular opportunities to decide.

- **Limits on Collection and Use:** Clear, enforceable standards should be established for both the *collection* and *use* of information on wearables and other Internet-connected devices. Users should be able to place limits on the data collected by and about them, specifying, for instance, that while their exercise, movements, and heart rate may be tracked, their locations may not. *No data* should be collected for ongoing processing until there is an affirmative expression from the consumer. Companies should get *specific* consent for every use, instead of attempting to encourage the consumer to agree to open-ended—and potentially unlimited—uses. There should be no "one-click" or "one-stop" consent systems that permit ongoing collection consumer data. There should be default limits on the uses of certain types of information, such as geolocation and biometric data.

- **Meaningful Disclosure:** Companies should be required to explain fully and in clear language what their data practices are, and there should be standardization of terminology so that comparisons are possible. Such clarifications should be designed to minimize customer confusion and maximize accountability. This information must reflect actual business practices or goals. If a company is unclear about its future plans for the data in question, it should not use the information beyond its initial purpose. If its business practices change in a manner that would impact a person's data, it should stop collection and use until a new informed consent is obtained. Companies should identify the third parties and service providers with whom they work, such as marketing clouds and data brokers, as well as any affiliates or subsidiaries that may have access to the health and wellness data that a company collects from consumers. They should also be required to make public disclosures about the operations of their data-analytic systems, including how they conceptualize and utilize algorithms.

- **Limited Sharing:** Wearable and other connected-health companies should not share user information with any third parties where advertising, marketing, or the promotion of other services are involved. Third parties should not provide

BEST PRACTICES AND NEXT STEPS

data on individuals to others (such as first-party sites, which may be health companies or social networks, etc.) without the knowledge and consent of an individual.

- **Consumer Access to Data:** Companies should make public their rationale and methodology for determining the criteria they use for consumer access to and correction and deletion of personal data. They should comply with requests for a person's data as soon as possible and at the lowest cost. There should be requirements ensuring that data can be corrected or deleted in a timely and pro-consumer manner.

- **Transparent anonymization:** The metrics used to determine how de-identification is most effectively accomplished should also be disclosed and subject to independent verification.

- **Usability testing:** In order to ensure that consumers are truly informed, wearable devices and apps should be tested to determine that consumers will be able to *understand* their privacy choices and terms of services. It is especially critical to ensure that judgments can be made under the conditions faced by many consumers—that they will be using a small screen, with competing applications, and may be "on-the-go." These studies should be made publicly available and updated regularly.

- **Broad-based standards:** Self-regulatory organizations should develop standards that apply to *all* sectors of the consumer connected-health industry, creating a more uniform and robust regime overall. There should be independent audits conducted to identify how effective a code or guidance is as it is applied in the actual marketplace.

- **Fair marketing practices:** The various participants in the digital health sector, including the wearable and mobile apps industry, should develop a set of fair marketing practices for using health-related data. These should include limits on problematic techniques, including many of those identified in this report. Of particular concern are techniques that enable discrimination on the basis of data related to ethnicity, gender, sexual orientation, age, community, or medical condition.

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 Affordable Care Act is very likely to undergo significant transformation, with millions of Americans facing the prospect of losing their health insurance or having their coverage severely cut. The potential of personal digital devices to reduce health care spending will likely play an important role in the policy debate. However, as this report documents, these technologies hold both promise and peril. In the absence of adequate safeguards, consumers and patients could face serious risks to their privacy and security, and also be subjected to discrimination and other harms. We have both an unprecedented opportunity and a moral obligation to broaden our national conversation around the goal of establishing a "Culture of Health," where "good health and well-being flourish across geographic, demographic, and social sectors," and "everyone has the opportunity to make choices that lead to healthy lifestyles."[262]

Acknowledgements

The authors would like to thank the following individuals for their help in the research and writing of this report: Linda Ackerman, Sammy Almashat, Khaliah Barnes, Cinnamon S. Bloss, Julie Brill, Michael Carome, Teresa Carr, Michelle De Mooy, Pam Dixon, Lori Dorfman, Jonathan Frankel, Gloria González Fuster, Claire Gartland, Robert Gellman, Beth Givens, Susan Grant, Cora Tung Han, Angela Hart, Deborah Hurley, Louisa Imperiale, Stuart Ingis, Megan Land, Bernard Lo, Jamie Love, Aleecia McDonald, Camille Nebeker, Janell Niederriter, Kevin Patrick, Deborah Peel, Jules Polonetsky, Manon Ress, Carolina Rossini, Marc Rotenberg, Mark A. Rothstein, John Simpson, Arthur D. Soto-Vásquez, Jay Stanley, Nicolas Terry, Lee Tien, David Vladeck, John Wilbanks, Isabelle Zaugg

Report design by Zak Bickel. Contributing illustrations by Matt Chase. Icons by Elias Stein. Photos by Jeff Elkins.

We would like to especially thank Paul Tarini of the Robert Wood Johnson Foundation for generously supporting our work on this issue.

CONTACT

Kathryn Montgomery, Ph.D.
Director, Communication Studies Division
Director, Doctoral Program in Communication
American University
kcm@american.edu

Jeff Chester, MSW
Executive Director
Center for Digital Democracy
jeff@democratucmedia.org

CENTER FOR DIGITAL DEMOCRACY

SCHOOL *of* COMMUNICATION
AMERICAN UNIVERSITY • WASHINGTON, DC

Bibliography and Appendices

Citations: Main Text

1. IBM, "Under Armour and IBM to Transform Personal Health and Fitness, Powered by IBM Watson," 6 Jan. 2016, https://www-03.ibm.com/press/us/en/pressrelease/48764.wss.

2. Endeavour Partners, "Inside Wearables—Part 3," Jan. 2016, http://endeavourpartners.net/white-papers/inside-wearables-part-3/.

3. comScore, "comScore Reports February 2016 U.S. Smartphone Subscriber Market Share," 6 Apr. 2016, https://www.comscore.com/Insights/Rankings/comScore-Reports-February-2016-US-Smartphone-Subscriber-Market-Share;Nielsen, "It's Thanksgiving, Please Pass the Smartphone," 24 November 2015, http://www.nielsen.com/us/en/insights/news/2015/its-thanksgiving-please-pass-the-smartphone.html; Quantified Self, "About the Quantified Self," http://quantifiedself.com/about/.

4. IMS Institute for Healthcare Informatics, "Patient Adoption of mHealth: Use, Evidence and Remaining Barriers to Mainstream Acceptance," Sept. 2015, http://www.imshealth.com/files/web/IMSH%20Institute/Reports/Patient%20Adoption%20of%20mHealth/IIHI_Patient_Adoption_of_mHealth.pdf. A recent report from Deloitte estimates that by 2015, over 500 million of a total 1.4 billion smart phone users worldwide will be using mHealth apps. And by 2018, 50 percent of the 3.4 billion mobile device users will have downloaded mHealth apps. Deloitte, "2016 Global Health Care Outlook: Battling Costs While Improving Care," 2016, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-2016-health-care-outlook.pdf. Ryan McAskill, "Global mHealth Market to Reach $49.12B by 2020," mHealth Intelligence, 10 Mar. 2015, http://mhealthintelligence.com/news/global-mhealth-market-to-reach-42.12b-by-2020.

5. "Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016," 2 Feb. 2016, http://www.gartner.com/newsroom/id/3198018; James Stables, "Fitness Trackers Are in a Race to the Bottom," Wareable, 16 June 2016, http://www.wareable.com/fitness-trackers/fitness-trackers-are-in-a-race-to-the-bottom; eMarketer, "Fitness Bands Still the Top Wearable in the U.S.," 27 May 2016, http://www.emarketer.com/Article/Fitness-Bands-Still-Top-Wearable-US/1014015; "US$ 24 Billion Worth of Wearable Medical Devices Expected to be Sold in 2016: Future Market Insights (FMI)," PR Newswire, 6 June 2016, http://www.prnewswire.com/news-releases/us-24-billion-worth-of-wearable-medical-devices-expected-to-be-sold-in-2016-future-market-insights-fmi-581986761.html; "The U.S. Consumer Wearables Market Will Reach $9.7B by 2019, Says Compass Intelligence," Market Wired, 20 Oct. 2015, http://www.marketwired.com/press-release/the-us-consumer-wearables-market-will-reach-97b-by-2019-says-compass-intelligence-2065369.htm.

6. "Samsung Addresses a Growing Mobile Health Market with Industry's First Smart Bio-Processor," 29 Dec. 2015, https://news.samsung.com/global/samsung-addresses-a-growing-mobile-health-market-with-industrys-first-smart-bio-processor.

7. For an overview of Fitbit's various health trackers, see Fitbit, "Fitbit Tracker Comparison," https://www.fitbit.com/compare.

8. Apple recently introduced its "Series 2" watch, which includes a GPS chip, enabling consumers to record their activity without relying on their mobile phone. Apple, "Apple Watch: Series 2," http://www.apple.com/apple-watch-series-2/.

9. Apple, "HealthKit," https://developer.apple.com/healthkit/.

10. Thync, http://www.thync.com.

11. Stacy Lawrence, "Khosla-backed Thync Dodges FDA, Heads to Market with $299 Mood-shifting Consumer Wearable," FierceMedicalDevices, 3 June 2015, http://www.fiercemedicaldevices.com/story/khosla-backed-thync-dodges-fda-heads-market-299-mood-shifting-consumer-wear/2015-06-03.

12. William H. Frist, "Connected Health and The Rise Of The Patient-Consumer," *Health Affairs* 33, n. 2 (Feb. 2014): 191-193, http://content.healthaffairs.org/content/33/2/191.full.

Citations: Main Text





13. Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: *A Revolution that Will Transform how we Live, Work, and Think* (New York: Houghton Mifflin Harcourt, 2013), p. 6. "The Big Data Conundrum: How to Define it?" MIT Technology Review, 3 Oct. 2013, http://www.technologyreview.com/view/519851/the-big-data-conundrum-how-to-define-it/; Svetlana Sicular, "Gartner's Big Data Definition Consists of Three Parts, Not to be Confused with Three 'V's," Forbes, 27 Mar. 2013, http://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/.

14. Teena Maddox, "Top IoT and Wearable Tech Trends for 2016: Smartwatches in Transition as Smartglasses Rule," TechRepublic, 14 Jan. 2016, http://www.techrepublic.com/article/top-iot-and-wearable-tech-trends-for-2016-smartwatches-in-transition-as-smartglasses-rule/.

15. Ericsson, "Wearable Technology and the Internet of Things: Internet of Wearable Things," https://www.ericsson.com/thinkingahead/consumerlab/consumer-insights/wearable-technology-and-the-internet-of-things#section_9.

16. Shane Mitchell, Nicola Villa, Martin Stewart-Weeks, and Anne Lange, "The Internet of Everything for Cities," Cisco, 2013, p. 2, http://www.cisco.com/web/about/ac79/docs/ps/motm/IoE-Smart-City_PoV.pdf.

17. "Digital Contact Lenses Can Transform Diabetes Care," The Medical Futurist, 7 Apr. 2015, http://medicalfuturist.com/2016/04/07/googles-amazing-digital-contact-lens-can-transform-diabetes-care/.

18. Consumers are showing increasing willingness to share data collected through digital devices with their medical practitioners, which can often be much more reliable than trying to recall such details during a brief doctor's appointment. Nathan Eddy, "Adoption of Health Apps, Wearable Devices Grows," eWeek, 5 Mar. 2016, http://www.eweek.com/small-business/adoption-of-health-apps-wearable-devices-grows.html. Research from the NIH has shown that when patients with heart disease and other chronic conditions were monitored remotely through mobile devices, the number of hospitalizations decreased sharply. Samsung, "Policy Gets Personal," *Washington Post,* 2015, http://www.washingtonpost.com/sf/brand-connect/samsung.

19. Caroline Chen and Shannon Pettypiece, "Target to Offer Fitbits to 335,000 Employees," Bloomberg Technology, 15 Sept. 2015, http://www.bloomberg.com/news/articles/2015-09-15/target-to-offer-health-tracking-fitbits-to-335-000-employees; Target, "Target Kicks off New Team Member Wellness Initiatives," A Bullseye View, 16 Sept. 2015, https://corporate.target.com/article/2015/09/team-member-wellness.

20. A.R. Doherty, P. Kelly, J. Kerr, S. Marshall, M. Oliver, H. Badland, A. Hamilton, and C. Foster, "Using Wearable Cameras to Categorise Type and Context of Accelerometer-identified Episodes of Physical Activity," *International Journal of Behavioral Nutrition and Physical Activity* 10 (13 Feb. 2013), http://www.ncbi.nlm.nih.gov/pubmed/23406270; M.M. Jankowska, J. Scjhippeerijm, and J. Kerr, "A Framework for Using GPS Data in Physical Activity and Sedentary Behavior Studies," *Exercise and Sport Sciences Review* 43, n. 1 (Jan. 2015): 48-56, http://www.ncbi.nlm.nih.gov/pubmed/25390297; J. Kerr, S.J. Marshall, S. Godbole, J. Chen, A. Legge, P. Kelly, M. Oliver, H.M. Badland, and C. Forster, (2013) "Using the SenseCam to Improve Classifications of Sedentary Behavior in Free-living Settings," *American Journal of Preventive Medicine* 44, n. 3 (Mar. 2013): 290-296, http://www.ncbi.nlm.nih.gov/pubmed/23415127.

21. Regina Greer-Smith, "Smartphone and Mobile Apps: An Important Solution to Increasing Participation and Engagement of Minority and Underserved Communities," Blog: National Partnership for Action, 22 Aug. 2013, http://minorityhealth.hhs.gov/npa/blog/BlogPost.aspx?BlogType=O&BlogID=2886.

22. Dan Munro, "Data Breaches in Healthcare Totaled Over 112 Million Records In 2015," *Forbes,* 31 Dec. 2015, http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#72f81067fd5a. Many consumers are already wary of the personal risks associated with these new digital devices. A 2014 PricewaterhouseCoopers survey of 1,000 consumers found that "82% of our respondents said they felt concerned that wearable technology would invade their privacy, and 86% indicated concern that wearables would make us more vulnerable to security breaches." PricewaterhouseCoopers, "The Wearable Future," Nov. 2014, https://www.pwc.com/mx/es/industrias/archivo/2014-11-pwc-the-wearable-future.pdf. A more recent study conducted by the Verizon Foundation found that while many consumers have downloaded health-related mobile apps, 46 percent have stopped using them, citing privacy as one of the major reasons. Paul Krebs and Dustin T. Duncan, "Health App Use Among US Mobile Phone Owners: A National Survey," *JMIR mHealth uHealth* 3, n. 4 (Oct.-Dec. 2015):e101, http://mhealth.jmir.org/2015/4/e101/#Introduction.

Citations: Main Text






23. As Nicolas Terry points out, "the HIPAA-HITECH model does not protect all health data. Rather, it only applies to certain forms of health data controlled by a limited group of data custodians. These covered entities are traditional, bricks-and-mortar providers, such as physicians, hospitals, pharmacies, health maintenance organizations, and health insurers. Thirteen years ago, that did not seem like a terrible policy decision. The storage and processing of petabytes of data were infeasible while the Internet and the World Wide Web were in their infancy and wearable computers and smartphones still seemed the stuff of science fiction. Today, however, vast amounts of medical data flow around in what may be termed 'HIPAA-free space,' essentially unregulated. This is true of what was once HIPAA data that were acquired by public health agencies and then sold and medically inflected data collected from transactions or social media interactions. It is also true of much of the health data curated by patients themselves, including personal health records (eg, blue button downloads from the Veterans Administration and the Centers for Medicare & Medicaid Services) or health-related data stored on smartphones or personal computers." Nicolas Terry, "Health Privacy is Difficult but Not Impossible in a Post-HIPAA Data-Driven World," *CHEST Journal* 146, n. 3 (2014): 835, doi:10.1378/chest.13-2909.

24. In October, 2016, the Federal Communications Commission (FCC), which regulates broadband Internet service providers, issued privacy rules that could potentially give consumers greater control over their online health data, however it remains unclear about whether the implementation of these new regulations will have an impact on data collection in the wearables marketplace. Federal Communications Commission, "FCC Adopts Broadband Consumer Privacy Rules," 27 Oct. 2016, https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules.

25. As part of this inquiry, we convened a one-day meeting in February 2016 with representatives from prominent privacy, civil liberties, health, and consumer-protection organizations to assess the major trends in the wearables marketplace, evaluate current regulatory and self-regulatory systems, and begin identifying the key building blocks for an effective public interest framework on consumer privacy and security in the wearables market. The meeting produced a number of important insights, and identified many issues that still needed to be researched. We have incorporated some of the input and feedback from the participants into this report.

26. The Federal IT strategic plan 1.0, "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap," was released in October 2015. One of its four "critical pathways" to accomplish this goal is for IT stakeholders to "coordinate…to promote and align consistent policies and business practices that support interoperability and address those that impede interoperability." It defines a "learning health system" as "an ecosystem where all stakeholders can securely, effectively and efficiently contribute, share and analyze data. A learning health system is characterized by continuous learning cycles, which encourage the creation of new knowledge that can be consumed by a wide variety of electronic health information systems." In addition to ensuring "health information is safe and secure," the Roadmap states that "stakeholders will also support greater transparency for individuals regarding the business practices of entities that use their data, particularly those are not covered by the HIPPA Privacy and Security rules, while considering the preferences of individuals." It also identifies key stakeholders who should play a role achieving its objectives, which include "individuals, consumers, patients… and professional organizations that represent these stakeholders' best interests." Office of the National Coordinator for Health Information Technology, "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap," version 1.0, https://www.healthit.gov/policy-researchers-implementers/interoperability. The Roadmap addresses a number important data governance and security issues as well, such as "consistent" data semantics and formats. The ONC has a "Blue Button" campaign promoting digital access by consumers to their health records. "Your Health Records: About Blue Button," HealthIT.gov, https://www.healthit.gov/patients-families/blue-button/about-blue-button.

27. "Federal Mandates for Healthcare: Digital Record-Keeping Requirements for Public and Private Healthcare Providers," USF Health, 20 June 2016, http://www.usfhealthonline.com/resources/healthcare/electronic-medical-records-mandate/#.V5RKxWWibFI.

28. See, for example, Venrock, "Portfolio," http://www.venrock.com/portfolio/; GV, "Portfolio: Life Science and Health," http://www.gv.com/portfolio/#life.

29. Sam Sutton, "Google Ventures Eyes Intersection of Healthcare, Data with Zephyr Investment–VCJ Deal News," The PE Hub Network, 21 Aug. 2015, https://www.pehub.com/2015/08/google-ventures-eyes-intersection-of-healthcare-data-with-zephyr-investment-vcj-deal-news/.

30. The other IPOs were MindBody, Evolent Health, Teladoc, and Invitae. Erica Garvin, "3 Digital Health Market Revelations to Watch in 2016," HIT Consultant, 4 Jan. 2016, http://hitconsultant.net/2016/01/04/30986/.

Citations: Main Text





31. The White House, "Precision Medicine Initiative: Guiding Principles for Protecting Privacy and Building Trust," https://www.whitehouse.gov/precision-medicine#section-principles; Sylvia Mathews Burwell and Lisa O. Monaco, "Precision Medicine Initiative and Data Security," White House Blog, 25 May 2015, https://www.whitehouse.gov/blog/2016/05/25/precision-medicine-initiative-and-data-security; White House Office of the Press Secretary, "FACT SHEET: Obama Administration Announces Key Actions to Accelerate Precision Medicine Initiative," 25 Feb. 2016, https://www.whitehouse.gov/the-press-office/2016/02/25/fact-sheet-obama-administration-announces-key-actions-accelerate; Jocelyn Kaiser, "NIH's 1-million-volunteer Precision Medicine Study Announces First Pilot Projects," *Science,* 25 Feb. 2016, http://www.sciencemag.org/news/2016/02/nih-s-1-million-volunteer-precision-medicine-study-announces-first-pilot-projects; Emily Wasserman, "Verily Tapped by NIH to Launch Obama's Precision Medicine Initiative," Fierce Biotech, 25 Feb. 2016, http://www.fiercemedicaldevices.com/story/verily-tapped-nih-launch-obamas-precision-medicine-initiative/2016-02-25. Data is to be collected from "a million-person cohort, from whom data of every conceivable kind—including genome, microbiome, epigenome—will be collected and stored in one colossal database, where scientists can access it for an endless array of studies and analyses." Jeneen Interlandi, "The Paradox of Precision Medicine," *Scientific American,* 1 Apr. 2016, http://www.scientificamerican.com/article/the-paradox-of-precision-medicine/. For a critical analysis of the privacy implications of the Precision Medicine Initiative, see https://www.worldprivacyforum.org/category/precision-medicine-initiative/.

32. National Cancer Institute, "Cancer Moonshot," http://www.cancer.gov/research/key-initiatives/biden-cancer-initiative. See also World Privacy Forum, "Precision Medicine Initiative," 17 May 2016, https://www.worldprivacyforum.org/category/precision-medicine-initiative/.

33. "Flatiron Health Raises $130 Million Series B Round Led by Google Ventures and Agrees to Acquire Leading Cloud-Based EMR Company Altos Solutions," 7 May 2014, https://flatiron.com/press/seriesB.

34. Google, "Google Fit," https://www.google.com/fit/; "Flatiron Health Raises $130 Million Series B Round Led by Google Ventures and Agrees to Acquire Leading Cloud-Based EMR Company Altos Solutions," 7 May 2014, http://flatiron.com/press/seriesB; Google, "Healthcare," Think with Google, https://www.thinkwithgoogle.com/topics/healthcare.html; Mark Bergen, "Verily, Google's Health Gambit, Is Stacked With Scientists. Now It Needs to Build a Business," re/code, 14 Dec. 2015, http://recode.net/2015/12/14/verily-googles-health-gambit-is-stacked-with-scientists-now-it-needs-to-build-a-business/; "Karen Ouk, Business Development Principal at Verily (Google Life Sciences)," https://www.linkedin.com/in/karenouk.

35. National Institutes of Health, "NIH Awards $55 Million to Build Million-person Precision Medicine Study," 6 July 2016, https://www.nih.gov/news-events/news-releases/nih-awards-55-million-build-million-person-precision-medicine-study.

36. PwC, "New Health Economy Vision for the Future," Dec. 2015, http://www.pwc.com/us/en/health-industries/healthcare-new-entrants.html.

37. See Kathryn C. Montgomery, "Safeguards for Youth in the Digital Marketing Ecosystem," in Dorothy G. Singer and Jerome L. Singer, eds., *Handbook of Children and the Media,* second edition (Thousand Oaks, CA: Sage Publications, 2011), pp. 631-648.

38. IAB, "U.S. Internet Ad Revenues Hit Landmark $59.6 Billion in 2015, a 20% Uptick Over Record-Breaking Numbers in 2014, Marking Sixth Consecutive Year of Double-Digit Growth," 21 Apr. 2016, http://www.iab.com/news/us-internet-ad-revenues-hit-landmark-59-6-billion-in-2015/; Juniper Research, "Digital Advertising Revenues to Double by 2020, Rising to $285Bn," 20 June 2016, http://www.juniperresearch.com/press/press-releases/digital-advertising-revenues-to-double-by-2020.

39. Information-technology scholar Zeynep Tufekci identifies six interconnected developments that are useful in addressing the impact of digital data on the public in the context of health: Big Data, emergent computational methods, Big-Data modeling, behavioral science modeling, experimental science in real-time environments, and the power of platforms and algorithmic governance. As Tufekci explains, the use of Big-Data techniques raises "questions of power, transparency and surveillance." Data today, she notes, now provide "more individualized profiling and modeling," involving "much greater data depth," and also "can be collected in an invisible, latent manner and delivered individually." Zeynep Tufekci, "Engineering the Public: Big Data, Surveillance and Computational Politics," *First Monday* 19, n. 7, 7 July 2014, http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097.

Citations: Main Text






40. Cooper Smith, "Reinventing Social Media: Deep Learning, Predictive Marketing, And Image Recognition Will Change Everything," Business Insider, 20 Mar. 2014, http://www.businessinsider.com/social-medias-big-data-future-2014-3.

41. C. Campbell, "Tracking Back-Talk in Consumer-Generated Advertising—An Analysis of Two Interpretative Approaches," *Journal of Advertising Research* 51, n. 1 (2011): 224; C. Murdough, "Social Media Measurement: It's Not Impossible," *Journal of Interactive Advertising* 10, n. 1 (2009): 94-99; C. Dăniasă, "The Mechanisms of the Influence of Viral Marketing in Social Media," *Economics, Management & Financial Markets* 5, n. 3 (Sept. 2010): 278-282; Gerd Leonhard, "Big Data, Big Business, Big Brother?" CNN, 26 Feb. 2013, http://edition.cnn.com/2014/02/26/business/big-data-big-business/. See also Joseph Turow, *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth* (New Haven: Yale University Press, 2013); Nick Couldry and Joseph Turow, "Advertising, Big Data, and the Clearance of the Public Realm," *International Journal of Communication* 8 (2014), 1710-1726; Tufekci, "Engineering the Public: Big Data, Surveillance and Computational Politics."

42. Natasha Singer, "Do Not Track? Advertisers Say 'Don't Tread on Us,'" *New York Times,* 13 Oct. 2012, http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html?_r=0.

43. Criteo, "Ovum Report: Future of E-commerce—The Road to 2026," http://www.criteo.com/media/4094/ovum-the-future-of-e-commerce-the-road-to-2026.pdf; Chuck Martin, "Tapping Wearables Data: 38% Of Marketers Want Daily Routine, 37% Precise Location," Media Post IoT Daily Connected Thinking, 28 Apr. 2016, http://www.mediapost.com/publications/article/274547/tapping-wearables-data-38-of-marketers-want-dail.html.

44. Criteo, "Ovum Report: Future of E-commerce—The Road to 2026."

45. U. S. Food and Drug Administration, "Keeping Watch Over Direct-to-Consumer Ads," http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm107170.htm.

46. Tracy Staton, "Pharma's Ad Spend Vaults to $4.5B, with Big Spender Pfizer Leading the Way," Fierce Pharma, 25 Mar. 2015, http://www.fiercepharma.com/dtc-advertising/pharma-s-ad-spend-vaults-to-4-5b-big-spender-pfizer-leading-way.

47. C. Lee Ventola, "Direct-to-Consumer Pharmaceutical Advertising: Therapeutic or Toxic?" *Pharmacy & Therapeutics* 36, n. 10 (Oct. 2011): 681-684, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3278148/.

48. eMarketer, "Health & Pharma Marketers Split Digital Spend Between Search, Display," 23 June 2016, http://www.emarketer.com/Article/Health-Pharma-Marketers-Split-Digital-Spend-Between-Search-Display/1014123.

49. Patricia Orsini, "The US Healthcare and Pharma Industry 2016," eMarketer, 12 May 2016, personal copy; Mike Snider, "Online Ad Spending to Top TV Ads in 2017," *USA Today,* 8 June 2016, http://www.usatoday.com/story/tech/news/2016/06/08/online-ad-spending-top-tv-ads-2017/85594160/.

50. Orsini, "The US Healthcare and Pharma Industry 2016."

51. For example, Merck's Aman Bhandari, who works on business developments and strategic partnerships, came from the White House, where he worked on technology issues.

52. Alexander Gaffney, "FDA Targets Companies for Facebook 'Likes.' Is Twitter Next?" RAPS, 12 Aug. 2014, http://www.raps.org/Regulatory-Focus/News/2014/08/12/20014/FDA-Targets-Companies-for-Facebook-Likes-Is-Twitter-Next/; "Strategic Pharma Solutions, Inc. Continues to Grow Digital Offerings through Expansion of Talent Base," 11 Sept. 2015, http://www.prnewswire.com/news-releases/strategic-pharma-solutions-inc-continues-to-grow-digital-offerings-through-expansion-of-talent-base-300141595.html?tc=eml_cleartime. Pharma and health companies, however, have been focused on digital marketing for a number of years. See, for example, "CDD, U.S. PIRG, Consumer Watchdog, and World Privacy Forum Call on FTC to Investigate Interactive Marketing of Pharmaceutical and Health Products and Services to Consumers and Health Professionals," 23 Nov. 2010, https://www.democraticmedia.org/sites/default/files/2010-11-investigate-pharma-marketing.pdf.

53. As the Electronic Privacy Information Center's website explains, "A drug manufacturer can pay a physician or a pharmacy to send refill reminders to patients, or to send information about a drug to all patients identified with a particular condition or taking particular medications. Although

Citations: Main Text





the drug manufacturer would not get PHI from the physician or pharmacy, it would accomplish the same marketing goals by paying someone else to promote its products. Furthermore, because the communication would come from an individual's physician or pharmacist, the information in the communication might be viewed as more trustworthy than it would be if it came from a drug manufacturer." Electronic Privacy Information Center, "Medical Record Privacy," https://www.epic.org/privacy/medical/.

54. Orsini, "The US Healthcare and Pharma Industry 2016"; Publicis Health, "Publicis Health Media," http://www.publicishealthcare.com/en/network/publicisHealthMedia.aspx.

55. "How Can Pharma Firms Market Their Way Back to Growth?" Knowledge @ Wharton, 27 Apr. 2016, http://knowledge.wharton.upenn.edu/article/how-can-pharma-firms-market-their-way-back-to-growth/.

56. "The most successful pharma marketing organizations do three things really well. They Discover the behaviors, beliefs, and needs of the people they are marketing to; they Design experiences relevant to the people they are marketing to; and they Deliver those experiences consistently, superbly, and efficiently. These phases are well known by experienced marketers, in pharma and elsewhere, but we refer to them as the 3Ds not only because they delineate the biggest areas of change for most companies, but also because we believe pharma needs to "think in 3D," adding depth and perspective as the industry moves from campaigns that talk at patients and physicians to solutions that *listen* to and *engage* with them." Wharton School, University of Pennsylvania; McKinsey and Company; and Google, *Pharma 3D: Rewriting the Script of Marketing in the Digital Age,* 2016, http://www.pharma3d.com/#chapter-856435. The book includes a case study from digital pharma marketing agency Intouch Solutions on how Baxalta, which produces drugs for hemophilia patients, successfully used Instagram (owned by Facebook) to promote its product. Instagram was selected because it is "one of the main channels on which young people communicate," with more than 400 million monthly users." Intouch Solutions, "Patient Engagement in the Instagram Generation: Going Where the Customer Is," Apr. 2016, https://dh1rvgpokacch.cloudfront.net/atavist/57222/document/raw/pharma3dint-1461021121-34.pdf.

57. "Pharma 3D: Wearables Can Lead to Unique Patient Insights and Engagement," https://dh1rvgpokacch.cloudfront.net/atavist/57222/document/raw/pharma3dwea-1461022903-75.pdf.

58. Orsini, "The US Healthcare and Pharma Industry 2016."

59. Welltok, "Products: CaféWell Concierge," http://welltok.com/products/cafewell-concierge.html.

60. "TapSense Launches Industry's First Programmatic Ad Platform for Apple Watch," 4 Jan. 2015, http://www.tapsense.com/blog/post/tapsense-launches-industrys-first-programmatic-ad-platform-apple-watch.

61. "Mindshare Launches Global Wearable Technology Unit," 10 July 2014, http://www.mindshareworld.com/news/mindshare-launches-global-wearable-technology-unit.

62. Under Armour, "Our Platform," http://advertising.underarmour.com/#platform; Under Armour, "MapMyFitness Virtual Fitness Challenge," http://advertising.underarmour.com/products/challenges/mapmyfitness-challenge; Under Armour, "Mobile Interstitials," http://advertising.underarmour.com/products/media/mobile-interstitial; Under Armour, "Our Products," http://advertising.underarmour.com/products/.

63. FitAd, "Technology," http://www.FitAd.com/technology.html.

64. "Partner Forum: Are Wearables a Pharma Field Day?" Medical Marketing & Media, 1 Aug. 2015, http://www.mmm-online.com/features/partner-forum-are-wearables-a-pharma-field-day/article/428202/; "Innovation in a Patient-Centric World," PharmaVOICE, July-Aug. 2015, http://www.pharmavoice.com/article/2015-pharmavoice100-innovation/.

65. Mayur Gupta, "Health Care Marketing Moves from Multichannel to Omnichannel," Ad Exchanger, 12 Nov. 2015, http://adexchanger.com/ad-exchange-news/health-care-marketing-moves-from-multichannel-to-omnichannel/.

66. Strap, "About Strap," https://www.straphq.com/company.

67. Strap, "Moving Beyond Basic Data: We Deliver Human Data Intelligence," https://www.straphq.com/; Strap, "The Three Step Process to Getting Started with Strap," https://www.straphq.com/resources/step-to-geing-started.

Citations: Main Text






68. eMarketer, "Wearable Usage Will Grow by Nearly 60% This Year," 28 Oct. 2015, http://www.emarketer.com/Article/Wearable-Usage-Will-Grow-by-Nearly-60-This-Year/1013159.

69. CMI, "New Native Ad Guidelines and What Steps You Need to Take," Jan. 2016, http://www.slideshare.net/CMI_Compas/new-native-advertising-guidelines-and-what-steps-you-need-to-take; Compass, Inc. "Insights," http://www.compasonline.com/insights; Coalition for Healthcare Communication, "FTC to Pharma on Native Advertising: Proceed with Caution," 18 Apr. 2016, http://www.cohealthcom.org/2016/04/18/ftc-to-pharma-on-native-advertising-proceed-with-caution/.

70. Under Armour, "Our Platform," http://advertising.underarmour.com/#platform; Under Armour, "MapMyFitness Virtual Fitness Challenge," http://advertising.underarmour.com/products/challenges/mapmyfitness-challenge; Under Armour, "Mobile Interstitials," http://advertising.underarmour.com/products/media/mobile-interstitial; Under Armour, "Our Products," http://advertising.underarmour.com/products/.

71. "FitAd Launches First-Ever Wearable Advertising Platform," Business Wire, 16 Dec. 2014, http://www.businesswire.com/news/home/20141216005211/en/FitAd-Launches-First-Ever-Wearable-Advertising-Platform; "FitAd," LinkedIn, https://www.linkedin.com/company/FitAd; FitAd, http://www.FitAd.com/.

72. An example of a wearable using haptic technology is the Hugshirt, which "records a hug like you would record a movie and deliver the data to your mobile via Bluetooth through a mobile App. You would obviously sense touch, warmth and emotion of the hug from a distant loved one." My Nguyen, "How New Haptic Wearable Devices Move Our Life," Wearable Technologies, 15 Sept. 2015, https://www.wearable-technologies.com/2015/09/how-new-haptic-wearable-devices-move-our-life/.

73. "What is Predictive Intelligence and How It's Set to Change Marketing in 2016," Smart Insights, 11 Feb. 2016, http://www.smartinsights.com/digital-marketing-strategy/predictive-intelligence-set-change-marketing-2016/.

74. Richie Etwaru, "How to Achieve Orchestrated Customer Engagement," PM360, 15 Dec. 2015, https://www.pm360online.com/how-to-achieve-orchestrated-customer-engagement/; IMS Health, "Orchestrated Customer Engagement: Orchestrate Every Customer Experience to Drive results. IMS Health. Sept. 2015, http://www.imshealth.com/en/solution-areas/technology-and-applications/orchestrated-customer-engagement; IMS Health, "IMS One," http://www.imshealth.com/en/solution-areas/technology-and-applications/ims-one/ims-one-intelligent-cloud.

75. Laurie Cutts, "Insider's Guide to Retargeting with Facebook Exchange," Nanigans, http://www.nanigans.com/2014/02/18/insiders-guide-to-facebook-exchange-ebook/.

76. "[T]his approach involves creating more personalized experiences based on the mix of data points you have on each customer. This can include classic demographic and psychographic segmentation elements along with other data points such as channel preference and past campaign response. Representing an extension of (and enhancement to) traditional market segmentation strategies, these microsegments are iteratively refined and improved based on new data as a campaign is executed." IMS Health, "The Healthcare Consumer Journey," 2015, http://www.imshealth.com/files/web/Global/Tech%20&%20Apps/Nexxus%20Commercial%20Application%20Suite/Nexxus%20Marketing/IMSH_Nexxus_Marketing_The_Healthcare_Communications_Journey_WP.pdf.

77. "Transformational Technology," Pharmaceutical Market Europe, May 2016, http://www.pmlive.com/digital_edition/pme/pharmaceutical_market_europe_-_may_2016; IMS Health, "Nexxus Commercial Application Suite," http://www.imshealth.com/en/solution-areas/technology-and-applications/nexxus; IMS Health, "Nexxus Marketing," http://www.imshealth.com/en/solution-areas/technology-and-applications/nexxus/nexxus-marketing; IMS Health, "IMS One."

78. Validic, "Our Company: About Us," https://validic.com/about.

79. Validic, "Our Difference," https://validic.com/our-difference; Stephanie Baum, "Validic Scoops Up Pfizer, Everyday Health as Clients for Data Aggregation Platform," MedCity News, 8 Dec. 2014, http://medcitynews.com/2014/12/validic-scoops-up-pfizer-everyday-health-as-clients-for-data-aggregation-platform/; "Validic and Omnicom Health Group Partner to Develop New Digital Health Communication Strategies and Solutions for Healthcare Companies Integrating Wearables and Biometric Data," 16 June 2016, http://www.prnewswire.com/news-releases/validic-and-omnicom-health-group-partner-to-develop-new-digital-health-communication-strategies-and-solutions-for-healthcare-companies-integrating-wearables-and-biometric-data-300285901.html?tc=eml_cleartime.

Citations: Main Text





80. Mikel Chertudi, "Strategic Marketing Plan Element #5: The Power of Personas," Adobe Digital Marketing Blog, 6 Oct. 2014, https://blogs.adobe.com/digitalmarketing/digital-marketing/strategic-marketing-plan-element-5-power-personas/; "Digilant Launches Consumer Persona Data Solution for Pinpointing New Audiences Programmatically," 16 June 2015, http://www.digilant.com/digilant-launches-consumer-persona-data-solution-for-pinpointing-new-audiences-programmatically/.

81. Crossix, "Consumer Database Propensity Scoring," http://www.crossix.com/solutions/consumer-database-scoring.aspx; Crossix, "Data-driven Consumer Profiles," http://www.crossix.com/Solutions/Consumer-Profiles.aspx.

82. LiveRamp, "Look alike Modeling: The What, Why, and How," http://liveramp.com/blog/look-alike-modeling-the-what-why-and-how/. A discussion of lookalike modeling on Facebook explains that "modeling an audience off of a closely related competitor—say, Pepsi modeling Coke's audience—can be a winning tactic. Simply target that company's fans, and you have an audience pretty much guaranteed to be interested in your product." Dillon Baker, "How to Use Facebook's Best Feature: Targeting," https://contently.com/strategist/2015/12/16/how-to-use-facebooks-best-feature-targeting/. See also Krux, "Lookalikes," http://www.krux.com/data-management-platform-solutions/lookalikes/; Sam Ransbotham, "Coca-Cola's Unique Challenge: Turning 250 Datasets Into One," *MIT Sloan Management Review,* 27 May 2015, http://sloanreview.mit.edu/article/coca-colas-unique-challenge-turning-250-datasets-into-one/.

83. Exelate, "25% of Advertisers Can't Define Lookalike Modeling," 30 Apr. 2014, http://exelate.com/resources/videos/25-advertisers-cant-define-lookalike-modeling/.

84. Skyhook, "SDK Data Previews," https://resources.skyhookwireless.com/wiki/type/documentation/context-accelerator/sdk-data-previews/3997879.

85. "4Info and Crossix Partnership Enables Pharma Brands to Deliver Mobile Ads Efficiently to Highly Qualified Audiences," 3 Mar. 2016, https://4info.com/Resources/Press-Releases/4INFO-and-Crossix-Partnership-Enables-Pharma-Brand. "Crossix does not use any actual medical data that would identify an individual as having a specific disease or condition; rather, it gathers information from healthcare data distributors and individual companies to gauge a consumer's propensity towards having an affliction based on over-the-counter drug purchases using loyalty cards, medical claims data indicating a doctor visit, and information from retail pharmacies showing prescription refills." Kate Kaye, "Data Partners to Tie Mobile Ads to Drug Refills, Doc Visits," *Advertising Age,* 3 Mar. 2016, http://adage.com/article/dataworks/data-partners-tie-mobile-ads-drug-refills-doc-visits/302937/. Crossix makes a similar claim of respect for privacy on behalf of its geo-targeting partner: "4INFO is able to identify specific audiences using household purchase history data so that national brand advertisers can reach precise audiences across mobile devices and desktops, and then measure campaign success based on actual sales lift. And we, too, do this while protecting the privacy of the consumer." Yet 4Info makes clear that its technology identifies "accurate audiences" regardless of the device used, "through linking devices and people using home address as a match key based on seeing devices over multiple days and times. Matched to Crossix data for ad delivery, we have found that audience accuracy/relevancy more than doubles compared to other platforms." Kirsten McMullen, "The Birth of Mobile Marketing for The Pharma Industry," 4Info Blog, 3 Mar. 2016, https://www.4info.com/Blog/2016-03/The-Birth-of-Mobile-Marketing-for-the-Pharma-Indus.

86. Skyhook, "SDK Data Previews."

87. Adprime also offers services to target via mobile and video platforms. Adprime Media, "Targeting," http://www.adprimemedia.com/advertisers/targeting.html; Adprime Media, "The Premier Ad Network," http://www.adprimemedia.com/advertisers/network_highlights.html.

88. AdRx, "Advertising Partnerships," http://www.adrxmedia.com/advertisers; AdRx, "Solutions," http://www.adrxmedia.com/solutions. AdRx also cites its membership in self-regulatory trade organizations, including the DAA (Digital Advertising Alliance) and NAI (Network Advertising Initiative), that it is "committed to brand safety" (but doesn't mention privacy). http://www.adrxmedia.com/brand-safety.

89. Malay Gandhi and Teresa Wang, "Digital Health Consumer Adoption: 2015," Rock Health, https://rockhealth.com/reports/digital-health-consumer-adoption-2015/#adoption; "How Can Pharma Firms Market Their Way Back to Growth?"

90. Monica Anderson, "Racial and Ethnic Differences in How People Use Mobile Technology," Pew Research Center FactTank, 30 Apr. 2015, http://www.pewresearch.org/fact-tank/2015/04/30/racial-and-ethnic-differences-in-how-people-use-mobile-technology/.

Citations: Main Text






91. Vertical Health, "Who We Work With," http://www.verticalhealth.com/who-we-work; Vertical Health, "What We Do," http://www.verticalhealth.com/what-we-do; Acxiom, "Partner Spotlight: Vertical Health," http://www.acxiom.com/partner-spotlight-verticalhealth/.

92. Virginia Lau, "Healthline Media Receives $95 Million in Equity Funding," Medical Marketing & Media, 15 Jan. 2016, http://www.mmm-online.com/media-news/healthline-media-receives-95-million-in-equity-funding/article/465375/; Healthline, "Advertise with Us," http://www.healthline.com/health/advertise-with-us; Healthline Mediakit, personal copy.

93. "WebMD Health Corp. (WBMD) SEC Filing 10-K Annual Report for the Fiscal Year Ending Thursday, December 31, 2015," https://www.last10k.com/sec-filings/wbmd; "In-Depth: How WebMD Navigated the Rise of Digital Health," Mobile Health News, 22 Jan. 2016, http://mobihealthnews.com/content/depth-how-webmd-navigated-rise-digital-health; http://www.fiercepharma.com/marketing/webmd-sees-rapid-online-and-mobile-growth-pharma-ads-more-to-come; WebMD, "WebMD Launches Health Improvement Program for iPhone® to Make Biometric Data Understandable and Actionable," 16 June 2014, http://investor.shareholder.com/wbmd/releasedetail.cfm?releaseid=854756&CompanyID=wbmd.

94. Robert Allen, "What is Programmatic Marketing?" Smart Insights, 8 Feb. 2016, http://www.smartinsights.com/internet-advertising/internet-advertising-targeting/what-is-programmatic-marketing/.

95. Liz Rowley, "Publicis Health Media Chief on Why Health is the Next Big Thing," Ad Exchanger, 10 Nov. 2014, http://adexchanger.com/agencies/publicis-health-medias-president-health-is-the-new-green/; "Programmatic Buying Stands to Disrupt Healthcare Marketing," Medical Marketing & Media, 1 Dec. 2014, http://www.mmm-online.com/features/programmatic-buying-stands-to-disrupt-healthcare-marketing/article/380332/. A Publicis marketing executive has also identified the possibilities for pharma companies to tap into their own data sources in order to "develop look-alike modeling" so new "patient" type prospects can be identified "at different moments throughout their patient pathway." Liz Rowley, "VivaKi, Publicis Health Media Take Health Care Advertising Programmatic," Ad Exchanger, 8 Oct. 2014, http://adexchanger.com/ad-exchange-news/vivaki-publicis-health-media-take-healthcare-advertising-programmatic/.

96. Everyday Health, "About Us: Our Portfolio," http://corporate.everydayhealth.com/about-us/default.aspx?section=portfolio. It also describes itself as the "21st Century advocates for consumers who want to live healthier, happier lives."

97. These data also help the company target other consumers through "predictive, lookalike modeling." Health Reach offers a suite of health-marketing applications, including "native mobile advertising solutions." Kirstin McQuigg, "Reaching Health Targets: It's Not Just in the Doctor's Office," Rauxa Blog, 6 May 2015, https://www.rauxa.com/who-we-are/news/blog/reaching-health-targets-its-not-just-in-the-doctors-office/; Everyday Health, "Advertise with Us," http://corporate.everydayhealth.com/advertise-with-us/default.aspx.

98. Xaxis, "A GeoMarketing Conversation with MoPub, Xaxis, VivaKi, and Factual," 10 Dec. 2014, https://www.xaxis.com/events/view/a-geomarketing-conversation-with-mopub-xaxis-vivaki-and-factual; "Xaxis Launches Light Reaction, Mobile-First Performance Business with Innovative Outcomes-Based Media Model," 2 June 2015, https://www.xaxis.com/press/view/xaxis-launches-light-reaction-mobile-first-performance-business-with-innova.

99. Quantcast, "Oracle Data Cloud," https://www.quantcast.com/audience-grid/data-partner/oracle-data-cloud-audience-data/; Quantcast, "Quantcast Audience Grid," https://www.quantcast.com/audience-grid/: Chris Lynch, "Bridge the Offline and Online Divide with New Oracle Marketing Cloud Features," Oracle Blog, 27 Oct. 2015, https://blogs.oracle.com/marketingcloud/bridge-the-offline-and-online-divide-with-new-oracle-marketing-cloud-features. Through the growth of "data append" services, companies are able to use offline transaction data to help drive online campaigns.

100. Merkle, "Connected Recognition," http://www.merkleinc.com/what-we-do/marketing-technology/merkle-data-management-cloud/connected-recognition#.Vzn-P0Gb-Bz8; "Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth,* Yale, 2011," Annenberg School for Communications, University of Pennsylvania, https://www.asc.upenn.edu/news-events/publications/joseph-turow-daily-you-how-new-advertising-industry-defining-your-identity.

101. Tom Ryan, "Has Mobile Created a New Marketing Moment of Truth?" CPGmatters, Oct. 2015, http://www.cpgmatters.com/RetailTrends101915.html.

Citations: Main Text





102. Tracking, according to one computer science scholarly paper, is the ability to "link activities performed by the same user in order to build detailed user profiles, learn users' interest, and better target their advertising." Sooel Son, Daehyeok Kim, Vitaly Shmatikov, "What Mobile Ads Know About Mobile Users," NDSS 2016, http://www.cs.cornell.edu/~shmat/shmat_ndss16.pdf; "The Difference Engine: The Spy in Your Pocket," *The Economist,* 29 Apr. 2011, http://www.economist.com/blogs/babbage/2011/04/mobile_tracking.

103. Glenn Warrington, "Tiles, Proxies and Exact Places: Building Location Audience Profiles," LinkedIn, 18 Nov. 2015, https://www.linkedin.com/pulse/tiles-proxies-exact-places-building-location-audience-warrington.

104. Google, "Understanding Advanced Location Options," AdWords Help, https://support.google.com/adwords/answer/1722038?hl=en; Facebook, "Helping Local Businesses Reach More Customers," Facebook for Business, 7 Oct. 2014, https://www.facebook.com/business/news/facebook-local-awareness; Facebook, "Ad Targeting Options," Facebook for Business, https://www.facebook.com/business/help/433385333434831.

105. FitAd, "Brands and Agencies," personal copy.

106. See, for example, Alteryx, "Alteryx Industry Solutions: Restaurants," https://www.alteryx.com/solutions/restaurants-analytics; Alteryx, "Alteryx Industry Solutions: Consumer Packaged Goods," https://www.alteryx.com/solutions/consumer-packaged-goods-analytics.

107. See, for example, Esri, "Esri Demographics: Explore Data," http://www.esri.com/data/esri_data/explore-data; ArcGIS, "Esri Demographics: Tapestry Segmentation," http://doc.arcgis.com/en/esri-demographics/data/tapestry-segmentation.htm; Geoscape, "Solutions: Geoscape Intelligence System," http://geoscape.com/solutions/geoscape-intelligence-system/.

108. Nielsen, "Location Mapping," https://www.claritas.com/sitereports/reports/demographic-maps/location-mapping.jsp.

109. Factual, "Solutions for Developers: Capabilities," https://www.factual.com/solutions/dsps-networks#capabilities.

110. R.J. Lewis, "Advertising Targeting for Healthcare & Life Sciences in the 21st Century," CBI Blog, 11 May 2015, http://blog.cbinet.com/blog/advertising-targeting-for-healthcare-life-sciences-in-the-21st-century.

111. eHealthcare Solutions, "Ad Specifications," http://www.ehealthcaresolutions.com/advertisers/media-buyers/ad-specifications/#advertisers; Remedy Health, a digital health platform that "helps over 200 million health consumers annually through various digital, mobile and point of care information products and technologies" has various sites, including HealthCentral, Diabetes Focus, Health After 50, and also works with BreastCancer.org, BerkeleyWellness.com, and others. Remedy Health Media, "Our Brands," http://www.remedyhealthmedia.com/brands-partners; Kevin McCaffrey, "Remedy Health Media Launches New Series: A Peek into Patients' Lives," Medical Marketing & Media, 15 June 2016, http://www.mmm-online.com/media-news/remedy-health-media-launches-new-series-a-peek-into-patients-lives/article/503104/.

112. Bill Jennings, "Can Programmatic Be Pharma-Friendly?" Media Post Marketing: Health, 9 Sept. 2015, http://www.mediapost.com/publications/article/257671/can-programmatic-be-pharma-friendly.html.

113. Tobi Elkin, "AccentHealth Acquires PageScience, A Programmatic Health Platform," Media Post Real-Time Daily, 14 June 2016, http://www.mediapost.com/publications/article/278100/accent-health-acquires-pagescience-a-programmatic.html.

114. PageScience, "Page-Level Targeting," http://www.pagescience.com. For additional information on how advances in data processing have transformed contextual advertising, see Judy Shapiro, "How to Navigate the Programmatic Contextual Maze," *Advertising Age,* 31 Aug. 2016, http://adage.com/article/digitalnext/navigate-programmatic-contextual-maze/305661/.

115. For example, in the retail and consumer goods industries, specialist companies such as Krux provide marketing profiles of customers and consumers created by data-management platforms and also incorporate a myriad of other information, including purchasing data from point-of-sale systems, credit-card transactions, and "hundreds of [third-party] data attributes." Sarah Sluis, "Nielsen Rolls Out Multitouch Attribution System Using Krux," Ad Exchanger, 6 May 2015, http://adexchanger.com/ad-exchange-news/nielsen-rolls-out-multitouch-attribution-system-using-krux/.

Citations: Main Text






116. "Health Media Network (HMN) Acquires the Rights to PetCARE TV, The Newest Addition to A Growing Point Of Care 'Family,'" 20 July 2016, http://www.hmnads.com/press-releases/health-media-network-hmn-acquires-rights-petcare-tv-newest-addition-growing-point-care-family/.

117. Health Media Network, "HMN Impact," http://www.hmnads.com/hmn_impact/.

118. Jim O'Dea, "The Pharmacy's New Role in Providing Healthcare Services," PM360, 23 Jan. 2014, https://www.pm360online.com/the-pharmacys-new-role-in-providing-healthcare-services/.

119. Shelfbucks, "The Future of Retailing...Brought to You by Shelfbucks," http://www.shelfbucks.com/complete-your-omni-channel-strategy. For example, General Mills, Coca-Cola, Pepsi, Kellogg's, and Nestle are clients of this tap and reward shopper marketing company. TPG Rewards, "TPG's Tap to Win Technology," http://taptopromo.com/; WireSpring Technologies, "POP Displays," https://www.wirespring.com/Solutions/pop_displays.html; Progressive Grocer, http://magazine.progressivegrocer.com/i/622765-jan-2016/97.

120. "Drugstores and Pharmacies," Mobile Commerce Daily, http://www.mobilecommercedaily.com/category/drugstores-pharmacies.

121. Walgreens, "Facts & FAQs," http://news.walgreens.com/fact-sheets/frequently-asked-questions.htm; Walgreens, "Balance Rewards," https://www.walgreens.com/balancerewards/balance-rewards.jsp.

122. The company lists 22 apps and 36 devices that can be connected with its Balance Rewards program. Walgreens, "Health Apps & Devices," https://www.walgreens.com/steps/appmarket.jsp.

123. Tim Baysinger, "Why This Broadcaster Is Going Beyond TV to Wearables and VR," *Adweek*, 20 Aug. 2015, http://www.adweek.com/news/television/why-broadcaster-going-beyond-tv-wearables-and-vr-166482.

124. Frank Adante, "Wearables Usher in the Next Evolution of Consumer Engagement," Inc., http://www.inc.com/frank-addante/wearables-usher-in-next-evolution-of-consumer-engagement.html.

125. Adobe tells clients to consider the "value [in] providing customers quick, simple and hyper-relevant updates and actions." These could include "breaking news headline, order status update or action, new personalized content available, and other contextual experiences (e.g. watch vibrating upon arrival of an Uber)." Carl Sandquist and Lakshmi Shivalingaiah, "The New Frontier: Measuring and Optimizing Wearables & Connected Devices," Adobe, 2016, personal copy. In early 2015 mobile advertising company TapSense announced the "first programmatic ad platform for the Apple Watch," featuring "interactive formats that go beyond banner, ads," including "watch faces, glances and full screen experiences"; "hyper-local targeting"; and "Apple Pay Integration," with "hyper-local coupons" that users can redeem "right from the convenience of their wrist," a practice that "reduces friction for the consumer." "TapSense Launches Industry's First Programmatic Ad Platform for Apple Watch." However, the company was immediately forced to pull back, after realizing that its advertising plans could potentially be blocked altogether because of Apple's development guidelines for its wearable devices. Daniel Eran Dilger, "TapSense Admits its Apple Watch 'Ad Platform' May Not Fly at All," AppleInsider, 6 Jan. 2015, http://appleinsider.com/articles/15/01/06/tapsense-admits-its-apple-watch-ad-platform-may-not-fly-at-all.

126. Britta O'Boyle, "What is Siri? Apple's Personal Voice Assistant Explained," Pocket-lint, 12 Oct. 2015, http://www.pocket-lint.com/news/112346-what-is-siri-apple-s-personal-voice-assistant-explained.

127. IBM, "The Weather Company Announces Watson Ads, To Humanize The Ad Experience for Consumers with Industry-First Capability," 2 June 2016, https://www-03.ibm.com/press/us/en/pressrelease/49858.wss; Google, "Google Brain Team," Research at Google, https://research.google.com/teams/brain/; Facebook, "Facebook Researchers Focus on the Most Challenging Machine Learning Questions at ICML 2016," Research at Facebook Blog, https://research.facebook.com/blog/facebook-researchers-focus-on-the-most-challenging-machine-learning-questions-at-icml-2016/; Christopher Heine, "IBM Watson Is Now Offering AI-Powered Digital Ads That Answer Consumers' Questions," *Adweek*, 2 June 2016, http://www.adweek.com/news/technology/ibm-watson-now-offering-ai-powered-digital-ads-answer-consumers-questions-171783; PHD Worldwide, "Our Views: 'Artificial Intelligence Will Change Consumer Decision-making Process" says PHD APAC's Chris Stephenson," 13 June 2016, http://www.phdmedia.com/newsartificial-intelligence-will-change-consumer-decision-making-process-says-chris-stephenson/; Babylon, "Everyone's Personal Health Service," http://www.babylonhealth.com/; Tom Sullivan, "Artificial

Citations: Main Text





Intelligence, Cognitive Computing and Machine Learning are Coming to Healthcare: Is it Time to Invest?" Healthcare IT News, 22 Apr. 2016, http://www.healthcareitnews.com/news/artificial-intelligence-cognitive-computing-and-machine-learning-are-coming-healthcare-it-time.

128. IBM, "Under Armour And IBM To Transform Personal Health and Fitness, Powered by IBM Watson," 6 Jan. 2016, https://www-03.ibm.com/press/us/en/pressrelease/48764.wss.

129. Under Armour, "Advertise on the Ultimate Health, Fitness & Nutrition Platform," http://advertising.underarmour.com/; Mark Bergen, "Under Armour Debuts 'Social Network for Activity,'" *Advertising Age,* 7 Jan. 2015, http://adage.com/article/consumer-electronics-show/armour-debuts-fitness-tracking-app/296479/.

130. Quoted in IBM, "The Weather Company Announces Watson Ads, To Humanize The Ad Experience for Consumers with Industry-First Capability," 2 June 2016, https://www-03.ibm.com/press/us/en/pressrelease/49858.wss.

131. Immersion, "Experience Haptics," http://www.immersion.com/experience-haptics/.

132. Immersion, "Wearables," http://www.immersion.com/wearables/; Immersion, "Haptic Enabling Kit for Wearable OEMs," http://www.immersion.com/products-services/touchsense-haptic-enabling-kit-for-wearables-oems/;Immersion, "Mobile Advertising," http://www.immersion.com/mobile-advertising/; Michael Essany, "Touch Technology Makes a Splash in Mobile Advertising," Mobile Marketing Watch, 10 June 2016, http://mobilemarketingwatch.com/touch-technology-makes-a-splash-in-mobile-advertising-67416/.

133. Affectiva, "Affectiva Overview," YouTube, https://www.youtube.com/user/affectiva; Affectiva, "The Mood-Aware Internet of Things," 24 July 2015, http://www.affectiva.com/blog/the-mood-aware-internet-of-things/.

134. Quoted in Roy Wallack, "Wearable Technology Catapulting Health and Fitness into Future," *Los Angeles Times,* 23 Jan. 2015, http://www.latimes.com/health/la-he-future-wearables-20150124-column.html.

135. David Champagne, Amy Hung, and Olivier Leclerc, "How Pharma Can Win in a Digital World," McKinsey & Company, Dec. 2015, http://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/how-pharma-can-win-in-a-digital-world.

136. "Minority Report—Personal Advertising in the Future," YouTube, 7 Dec. 2010, https://www.youtube.com/watch?v=7bXJ_obaiYQ.

137. Pam Dixon, "A Brief Introduction to Fair Information Practices," World Privacy Forum, Jan. 2008, https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

138. Deborah Hurley, "Taking the Long Way Home: The Human Right of Privacy," in Marc Rotenberg, Julie Horwitz, and Jeramie Scott, eds., Privacy in the Modern Age (New York: The New Press, 2015), pp. 70-77; Robert Gellman, "Fair Information Practices: A Basic History," Social Science Research Network, 17 June 2016, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020.

139. Hurley, "Taking the Long Way Home: The Human Right of Privacy."

140. "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes," staff report for Chairman Rockefeller, Senate Committee on Commerce, Science, and Transportation, 18 Dec. 2013, https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf; Daniel J. Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," 114 *Columbia Law Review* 583 (2014), http://ssrn.com/abstract=2312913; Colin J. Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" in Phillip E. Agre and Marc Rotenberg, eds, *Technology and Privacy: The New Landscape* (Cambridge, MA: MIT Press, 1997), p. 113.

141. Deborah Peel, "An Implementation Path to Meet Patients' Expectations and Rights to Privacy and Consent," in Linda Koontz, ed., *Information Privacy in the Evolving Healthcare Environment* (Chicago: Healthcare Information and Management Systems Society, 2013), pp. 89-116. Electronic Frontier Foundation, "The Law and Medical Privacy," https://www.eff.org/issues/law-and-medical-privacy. The Health Information Technology for Economic and Clinical Health Act (HITECH), which was passed in 2009 as part of the omnibus economic stimulus package, included stronger security provisions for protected health information covered under HIPAA. For example, the law

Citations: Main Text

toughened data-breach-notification laws, imposing larger fines, requiring more extensive public notifications when data are lost, and extending the provisions to the business associates of health-care providers. Marci Meingast, Tanya Roosta, and Shankar Sastry, "Security and Privacy Issues with Health Care Information Technology," *Conference Proceedings of the IEEE Engineering in Medicine and Biology Society* 1 (2006): 5453-8, http://www.cs.jhu.edu/~sdoshi/jhuisi650/discussion/secprivhealthit.pdf; Howard Anderson, "The Essential Guide to the HITECH Act," Information Security Media Group, 8 Feb. 2010, http://www.healthcareinfosecurity.com/essential-guide-to-hitech-act-a-2053/op-1; "How the HITECH Act Changes HIPAA Compliance," SearchHealthIT, http://searchhealthit.techtarget.com/tip/How-the-HITECH-Act-changes-HIPAA-compliance.

142. Nicolas Terry, "Protecting Patient Privacy in the Age of Big Data," *University of Missouri-Kansas City Law Review* 81, no. 2 (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2153269.

143. Latanya Sweeney, "Only You, Your Doctor, and Many Others May Know," *Technology Science,* 29 Sept. 2015, http://techscience.org/a/2015092903/.

144. Nicolas Terry, "Big Data Proxies and Health Privacy Exceptionalism," *Health Matrix—Journal of Law-Medicine* 24 (2014): 65-108, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320088#%23.

145. Terry, "Protecting Patient Privacy in the Age of Big Data."

146. According to industry trade reports, many companies in the consumer-wearables market appear to be wary of forming any partnerships with HIPAA-covered entities, specifically to avoid having to comply with the law's privacy and security rules. Kristen Lee, "Wearable Health Technology and HIPAA: What Is and Isn't Covered," SearchHealthIT, http://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered.

147. U.S. Department of Health and Human Services, "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA," https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

148. Colin Lecher, "The FDA Doesn't Want to Regulate Wearables, and Device Makers Want to Keep It That Way," The Verge, 24 June 2015, http://www.theverge.com/2015/6/24/8836049/fda-regulation-health-trackers-wearables-fitbit.

149. U.S. Food and Drug Administration, "Webinar— Final Guidance on 'General Wellness: Policy for Low-Risk Devices,'" 1 Sept. 2016, http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm515955.htm.

150. The Federal Communications Commission is beginning to play an important privacy role, as a result of its 2015 decision on "network neutrality. Through its enforcement of Title II of the Communications Act, the FCC now has the authority to ensure that broadband Internet service providers (ISPs) protect the privacy of subscriber data used for commercial purposes. The commission also proposed a plan for ISP privacy in 2016. Federal Communications Commission, "FCC Adopts Strong, Sustainable Rules to Protect the Open Internet," https://www.fcc.gov/document/fcc-adopts-strong-sustainable-rules-protect-open-internet; Federal Communications Commission, "FCC Releases Proposed Rules to Protect Broadband Consumer Privacy," 1 Apr. 2016, https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy.

151. Joseph Turow, "Americans and Online Privacy: The System is Broken," Annenberg Public Policy Center of the University of Pennsylvania, June 2003, http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.

152. Cooper J. Spinelli, "Far From Fair, Farther From Efficient: The FTC and the Hyper-Formalization of Informal Rulemaking," *Legislation and Policy Brief* 6, n. 1, Article 3 (2014), http://digitalcommons.wcl.american.edu/lpb/vol6/iss1/3; David A. Balto, "Bring the FTC into the 21st Century," *The Hill,* 4 May 2010, http://thehill.com/opinion/op-ed/95947-bring-the-ftc-into-the-21st-century.

153. Federal Trade Commission, "Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises," 29 Nov. 2011, http://ftc.gov/opa/2011/11/privacysettlement.shtm.

154. As the report explained, "For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes." Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," Mar. 2012, pp. 59-60, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

Citations: Main Text





155. Kate Kaye, "FTC: Fitness Apps Can Help You Shred Calories—and Privacy," *Advertising Age,* 7 May 2014, http://adage.com/article/privacy-and-regulation/ftc-signals-focus-health-fitness-data-privacy/293080/. "FTC Examines Benefits and Risks of Consumer Generated and Controlled Health Data," Chronicle of Data Protection, 9 May 2014, http://www.hldataprotection.com/2014/05/articles/consumer-privacy/ftc-examines-benefits-and-risks-of-consumer-generated-and-controlled-health-data-2/.See also Sweeney, "Only You, Your Doctor, and Many Others May Know."

156. Federal Trade Commission, "Internet of Things—Privacy & Security in a Connected World," FTC Staff Report, Jan. 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

157. Michelle De Mooy, "Guidance but Not Direction: The FTC Tool for Mobile Health App Developers," CDT Blog,8 Apr. 2016, https://cdt.org/blog/guidance-but-not-direction-the-ftcs-tool-for-mobile-health-app-developers/.

158. "COPPA—Children's Online Privacy Protection Act," https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule. The authors of this report led the coalition that pushed for passage of COPPA during the 1990's and have been involved in regulatory proceedings and Congressional hearings regarding law's implementation since it was passed in 1998. For a case history of COPPA's passage, see Kathryn C. Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (Cambridge, MA: MIT Press, 2007), pp. 67-106.

159. Several years ago, at the urging of child advocates, consumer organizations, and privacy groups, the FTC conducted a comprehensive review of the COPPA rules, releasing a revised set of regulations that update and clarify COPPA's basic safeguards. These new regulations, which became effective in 2013, add new protections specifically designed to address a wide range practices on social media, mobile, and other platforms. Federal Trade Commission, "FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information by Amending Children's Online Privacy Protection Rule," 19 Dec. 2012, http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

160. Federal Trade Commission, "FTC Issues Final Breach Notification Rule for Electronic Health Information," 17 Aug. 2009, https://www.ftc.gov/news-events/press-releases/2009/08/ftc-issues-final-breach-notification-rule-electronic-health.

161. The rule applies to vendors of personal health records that provide online repositories, enabling patients to access their own medical information, as well as to companies offering third-party applications for personal health records. The latter category includes "devices such as blood pressure cuffs or pedometers whose readings consumers can upload into their personal health records." As explained in a recent health law professional journal, "the FTC Health Breach Notification Rule regulates breaches, not purposes for which health data may be used as does HIPAA. The FTC rule also does not prevent the sale of user health data. Similarly, the FTC rule does not require health apps to seek clear and unambiguous consent for uses or disclosures that consumers would not typically expect. When compared to HIPAA regulation, Congress's mandate to the FTC to protect electronic health records leaves many privacy and security concerns unaddressed." Hank Creasy and David Knoespel, "The New Generation of Electronic Health Records: What Health Apps Know About You," *Virginia Lawyer* 64 (June 2015): 24-25, http://www.vsb.org/docs/valawyermagazine/vl0615-health-records-apps.pdf.

162. Federal Trade Commission, "FTC Cracks Down on Marketers of 'Melanoma Detection' Apps," 23 Feb. 2015, https://www.ftc.gov/news-events/press-releases/2015/02/ftc-cracks-down-marketers-melanoma-detection-apps.

163. Solove and Hartzog, "The FTC and the New Common Law of Privacy."

164. Solove and Hartzog, "The FTC and the New Common Law of Privacy."

165. Danny Yadron, "America's Top Privacy Regulator Refuses to Wear a Fitbit," The Guardian, 6 Jan. 2016, https://www.theguardian.com/technology/2016/jan/06/fitbit-ces-privacy-concerns-health-step-counter-technology.

166. Federal Communications Commission, "FCC Adopts Broadband Consumer Privacy Rules."

167. The White House, "We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online," 23 Feb. 2012, http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

Citations: Main Text

168. Lan Du, "White House Releases Administration Discussion Draft for Consumer Privacy Bill of Rights Act of 2015," 23 Mar. 2015, http://jolt.law.harvard.edu/digest/privacy/white-house-releases-administration-discussion-draft-for-consumer-privacy-bill-of-rights-act-of-2015; Center for Democracy and Technology, "Coalition Letter to President Regarding Consumer Privacy Bill of Rights," 3 Mar. 2015, https://cdt.org/insight/coalition-letter-to-president-regarding-consumer-privacy-bill-of-rights/; "The President's Weak Privacy Proposal," *New York Times,* 6 Mar. 2015, http://www.nytimes.com/2015/03/06/opinion/the-presidents-weak-privacy-proposal.html?_r=0.

169. William Kovacs, "Administration's Privacy Legislation Would Cost Americans Jobs," Above the Fold, 23 Mar. 2015, https://www.uschamber.com/above-the-fold/administrations-privacy-legislation-would-cost-americans-jobs.

170. Zach Miners, "Internet 'Do Not Track' System is in Shatters," *Computerworld,* 22 May 2014, http://www.computerworld.com/article/2489727/data-privacy/internet--do-not-track--system-is-in-shatters.html; Ed Bott, "Why Do Not Track is Worse than a Miserable Failure," ZDNet, 21 Sept. 2012, http://www.zdnet.com/why-do-not-track-is-worse-than-a-miserable-failure-7000004634/; Fred B. Campbell, Jr., "The Slow Death of 'Do Not Track,'" *New York Times,* 26 Dec. 2014, http://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html.

171. There are other organizations that work to help companies comply with regulatory and self-regulatory privacy requirements. TRUSTe, a "Data Privacy Management" company, helps its members "safely collect and use customer data." The group conducts assessments, implements "compliance controls," and engages in ongoing monitoring. TRUSTe's "Certified Privacy Seal" is designed to inform consumers and others that a company is engaging in responsible data practices. It created an Internet of Things Working Group in 2014. TRUSTe, "About TRUSTe," https://www.truste.com/about-truste/; "Xiaomi Demonstrates Commitment to Privacy Through Partnership with TRUSTe for Privacy Assessment Technology and Certification Services," 10 May 2016, https://www.truste.com/about-truste/press-room/xiaomi-demonstrates-commitment-privacy-partnership-truste-privacy-assessment-technology-certification-services/; "TRUSTe Announces Multi-Stakeholder IoT Privacy Tech Working Group as Next Step to Help Enhance Consumer Privacy in Internet of Things," Business Wire, 11 July 2014, http://www.prnewswire.com/news-releases/truste-announces-multi-stakeholder-iot-privacy-tech-working-group-as-next-step-to-help-enhance-consumer-privacy-in-internet-of-things-266742251.html. The Mobile Marketing Association (MMA) represents hundreds of global companies working to advance mobile marketing and advertising. MMA issued its own guidance on mobile app privacy in 2012, but also supports the Digital Advertising Alliance (DAA) self-regulatory system. Mobile Marketing Association, "Privacy," http://www.mmaglobal.com/programs/privacy; "Mobile Marketing Association Releases Final Privacy Policy Guidelines for Mobile Apps," 24 Jan. 2012, http://www.mmaglobal.com/news/mobile-marketing-association-releases-final-privacy-policy-guidelines-mobile-apps. There is also a new organization called the Trustworthy Accountability Group (TAG), which offers a seal (TAG-ID) to identify that its members engage in reputable online ad practices. TAG addresses issues related to malware, online fraud, and piracy, and fights "criminal activity in the online advertising food chain." Trustworthy Accountability Group, https://tagtoday.net/.

172. Digital Advertising Alliance, "YourAdChoices Gives You Control," http://youradchoices.com.

173. However, if drug prescriptions or medical records have undergone a de-identification process approved by the HIPAA Privacy rule, they are exempted from any DAA safeguards. As we explain in the section on current digital marketing practices for health products and services, the so-called "HIPAA-compliant records" permit a growing array of ways to target an individual.

174. A number of DAA member companies engage in various forms of health marketing. They include Audience Partners, Conversant, and Medicx. The NAI's members include companies also involved in forms of health advertising, such as Oracle's BlueKai, Conversant, MaxPoint, TubeMogul, and Videology. The MMA membership includes Cancer Centers of America, which engages in a broad range of digital marketing practices, as well as IBM's The Weather Company (which is now using Watson's predictive ad technology). The DAA's mobile app—called AppChoices—used by consumers, lists several dozen companies where users can "opt-out" of having their data collected for behaviorally targeted marketing. Consumers are unlikely to realize that RUN, an ad-targeting company whose opt-out is offered on AppChoices, works with health marketer Crossix, and that they can be targeted as a "likely prescription type" for diabetes, Parkinson's, multiple sclerosis, cancer, obesity, migraine, etc.

175. Network Advertising Initiative, "The NAI Code of Conduct," http://www.networkadvertising.org/code-enforcement/code.

176. Network Advertising Initiative, "Sensitive Data," https://www.networkadvertising.org/glossary/term/sensitive-data.

Citations: Main Text

177. Anthony Matyjas, "NAI Leading the Way on High Standards for Health Data," Network Advertising Initiative Blog, 31 Oct. 2014, https://www.networkadvertising.org/blog/nai-leading-way-high-standards-health-data.

178. As the guidelines read, "The disclosure may be in, or linked from, the member's privacy policy, in other consumer-facing materials, such as a preference manager, or in another location on the member's website that is reasonably easy for users to find." Companies must disclose what is called "sensitive health segments" that they may use (which includes cancer, mental health conditions, and sexually transmitted diseases), and also "non-sensitive" topics (which are "such general health categories" as headaches, allergies, diet, fitness, and skin care). There are also practices involving the creation of specialized categories for health marketing that only trigger a requirement that members "disclose a representative sample" of what NAI calls "custom segments," or provide an explanation of how they use such data. See especially the 2015 update to the NAI code. Noga Rosenthal, "2015 Update to the NAI Code," Network Advertising Initiative Blog, 14 May 2015, https://www.networkadvertising.org/blog/2015-update-nai-code. In its code applying to mobile applications and health, the NAI says that it exempts "some data sources, such as data collected offline and integrated for targeted advertising across websites or app" from having to comply with its code. In a blog post, NAI explains that "those practices thus fall outside of our current enforcement efforts unless an NAI member has voluntarily committed to adhere to our Opt-In requirement for Sensitive Data regardless of the data source.... NAI encourages all NAI member companies to apply the NAI Code and App Code's Sensitive Data principles to all user-level targeted advertising across unaffiliated web domains or mobile applications, even if the source of that data is not currently covered by the NAI Code and App Code." Network Advertising Initiative, "Starting Points for Sensitive Data: NAI Requirements and Best Practices for Health-Related Targeting," Network Advertising Initiative Blog, 15 Jan. 2016, https://www.networkadvertising.org/blog/starting-points-sensitive-data-nai-requirements-and-best-practices-health-related-targeting.

179. Consumer Technology Association, "Association Unveils First-of-Its-Kind, Industry Supported Principles on Wellness Data Privacy," 26 Oct. 2015, https://www.cta.tech/News/Press-Releases/2015/October/Association-Unveils-First-of-Its-Kind,-Industry-Su.aspx. In addition to overseeing its recently released privacy and security principles for personal wellness data, CTA also conducts research on the heart and fitness technology market. Members of the division's board include representatives from Fitbit, AT&T, Qualcomm, Misfit, Walgreens, Validic, and Google, among others. Consumer Technology Association, "Health and Fitness Technology Division," https://www.cta.tech/Membership/Divisions-Councils/Health-and-Fitness-Technology-Division.aspx.

180. Consumer Electronics Association, "Guiding Principles on the Privacy and Security of Personal Wellness Data," 20 Oct. 2015, https://fpf.org/wp-content/uploads/2015/10/CEA-Guiding-Principles-on-the-Privacy-and-Security-of-Personal-Wellness-Data-102215.pdf.

181. The trade group also says that "A company should not knowingly use or disclose personal wellness data in ways that are likely to be unjust or prejudicial to consumers' eligibility for, or access to, employment, healthcare, financial products or services, credit, housing or insurance." However, under its "Data Review, Correction, and Deletion" provisions, it appears that data can be used to "determine the user's eligibility for, or access to, employment, healthcare, financial products or services, credit, housing or insurance." All that is required to do so is to provide a "user with a means to review and correct the company's stored personal wellness data." That provision has several exemptions, including whether the deletion is technically, economically, and legally feasible; whether the company can attribute personal wellness data to the requesting user; and that the user does not already have the ability to delete his or her personal wellness data. Companies are encouraged to develop "concise" notices that summarize their wellness-data practices, including through the use of "creative formats"—such as video, icons, or graphics—that "facilitate rapid learning" of their procedures. It also calls on companies to use their privacy policies to inform users how they respond to requests from law and civil enforcement agencies. Consumer Electronics Association, "Guiding Principles on the Privacy and Security of Personal Wellness Data," p. 3.

182. As explained in a footnote, "These Principles do not endorse any particular method of de-identification or set a standard for when data has been adequately de-identified. Instead, companies should use their expertise, taking into account the type and use of personal wellness data and using the technical tools available to them, to determine how to de-identify such data." Consumer Electronics Association, "Guiding Principles on the Privacy and Security of Personal Wellness Data," p. 2.

Citations: Main Text






183. Consumer Technology Association, "Association Unveils First-of-Its-Kind, Industry Supported Principles on Wellness Data Privacy."

184. Melanie Bates, "Mobile Apps Study Underscores Necessity of Strong Best Practices for Health and Wellness Data," Future of Privacy Forum, 17 Aug. 2016, https://fpf.org/2016/08/17/best-practices-consumer-wearables-wellness-apps-devices/; Future of Privacy Forum, "Supporters," https://fpf.org/about/supporters/.

185. Future of Privacy Forum, "About Consumer Wellness & Wearables," https://fpf.org/issues/consumer-wellness-wearables/.

186. Bates, "Mobile Apps Study Underscores Necessity of Strong Best Practices for Health and Wellness Data." See also Christopher Wolf, Jules Polonetsky, Kelsey Finch, "A Practical Privacy Paradigm for Wearables," Future of Privacy Forum, 8 Jan. 2015, https://fpf.org/wp-content/uploads/FPF-principles-for-wearables-Jan-2015.pdf. FPF has received a grant from the Robert Wood Johnson Foundation for its health wearable privacy work.

187. Future of Privacy Forum, "Best Practices for Consumer Wearables & Wellness Apps & Devices," 17 Aug. 2016, p. 4, https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf.

188. All the data collected for so-called "non-medical lifestyle wellness purposes" can be used for digitally "tailored" behavioral advertising on mobile devices, personal computers, and even digital TVs. The only safeguard offered is an "opt-out," essentially permitting what are known as "first parties"—the companies with which you are or have had direct interactions—to engage in ongoing monitoring and targeting of an individual for health or medical marketing. Companies do not need consent in order to share consumer data with their partners or vendors that provide data analytics or other information services. While these companies are expected to follow contractual obligations, including "limitations on data uses," consumers are given no assurances of what those limits are. Future of Privacy Forum, "Best Practices for Consumer Wearables & Wellness Apps & Devices."

189. Online Trust Alliance, "About Us," https://otalliance.org/about-us; Online Trust Alliance, "Industry Best Practices," https://otalliance.org/best-practices/industry-best-practices.

190. Online Trust Alliance, "Internet of Things," https://otalliance.org/initiatives/internet-things.

191. Craig Spiezle, "Creating Trust for the Internet of Things," Online Trust Alliance, 13 July 2016, https://otalliance.org/system/files/files/resource/documents/ota-_iot_trust_framework.pdf.

192. Online Trust Alliance, "IoT Resources," https://otalliance.org/resources/iot-resources.

193. Online Trust Alliance, "IoT Trust Framework—Resource Guide," 8 Apr. 2016, https://otalliance.org/system/files/files/in-the-news/images/iot_trust_resource_guide_4-8.pdf; Online Trust Alliance, "Internet of Things"; Sean Lyngaas, "Report: UL in Talks with White House on IoT certification," FCW, 7 July 2015, https://fcw.com/articles/2015/07/07/ul-iot-cert.aspx; The White House, "FACT SHEET: Cybersecurity National Action Plan," 9 Feb. 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

194. Digital Advertising Alliance, "DAA Self-Regulatory Principles," http://digitaladvertisingalliance.org/principles; Wendy Davis, "NAI Issues Privacy Guidelines For Digital Fingerprinting, Other Non-Cookie Ad Technology," Media Post Daily Online Examiner, 19 May 2015, http://www.mediapost.com/publications/article/250297/nai-issues-privacy-guidelines-for-digital-fingerpr.html; Wendy Davis, "BBB Warns Publishers To Comply With Privacy Rules," Media Post Daily Online Examiner, 19 Oct. 2013, http://www.mediapost.com/publications/article/211260/bbb-warns-publishers-to-comply-with-privacy-rules.html.

195. Wendy Davis, "Aetna and Sega Violated Industry's Mobile Privacy Code, Watchdog Says," Media Post Daily Online Examiner, 14 July 2016, http://www.mediapost.com/publications/article/280330/; Advertising Self-Regulation Council, "Accountability Program Decisions, Dispositions, Closures, and Guidance," http://www.asrcreviews.org/accountability-program-decisions/.

196. Robert Gellman and Pam Dixon, "Many Failures: A Brief History of Privacy Self-Regulation in the United States," World Privacy Forum, 14 Oct. 2011, http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf; Chris Hoofnagle, "Privacy Self-Regulation: A Decade of Disappointment," Electronic Privacy Information Center, 4 Mar. 2005, http://epic.org/reports/decadedisappoint.html; Center for Digital Democracy, "U.S. Online Data Trade Groups

Citations: Main Text





Spin Digital Fairy Tale to USTR about US Consumer Privacy Prowess—CDD Says Privacy Out of Bounds in TTIP," 29 May 2013, https://www.democraticmedia.org/content/us-online-data-trade-groups-spin-digital-fairy-tale-ustr-about-us-consumer-privacy-prowess.

197. Eric Topol, *The Patient Will See You Now: The Future of Medicine Is in Your Hands* (New York: Basic Books, 2015); Alex Pentland, Todd G. Reid, and Tracy Heibeck, "Big Data and Health: Revolutionizing Medicine and Public Health," a report of the Big Data and Health Working Group, 2013, https://kit.mit.edu/sites/default/files/documents/WISH_BigData_Report.pdf.

198. Deborah Estrin and Ari Juels, "Reassembling Our Digital Selves," *Daedelus* 145, n. 1 (Winter 2016): 43-53.

199. UC Berkeley Center for Long-Term Cybersecurity, "Scenario Four: Intentional Internet of Things," https://cltc.berkeley.edu/scenario/scenario-four/.

200. NORC at the University of Chicago, "Understanding the Impact of Health IT in Underserved Communities and those with Health Disparities," The Office of the National Coordinator for Health Information Technology Department of Health and Human Services," May 2013, https://www.healthit.gov/sites/default/files/hit_disparities_report_050713.pdf.

201. Upturn, "Civil Rights, Big Data, and Our Algorithmic Future," Sept. 2014, https://bigdata.fairness.io/wp-content/uploads/2015/04/2015-04-20-Civil-Rights-Big-Data-and-Our-Algorithmic-Future-v1.2.pdf; National Science and Technology Council, "National Privacy Research Strategy," June 2016, https://www.whitehouse.gov/sites/default/files/nprs_nstc_review_final.pdf.

202. Electronic Frontier Foundation, "The Law and Medical Privacy."

203. See Joseph W. Jerome, "Buying and Selling Privacy: Big Data's Different Burdens and Benefits," *Stanford Law Review* 47, 3 Sept. 2013.

204. Joseph Turow and Nora Draper, "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation," Annenberg School for Communications, University of Pennsylvania, https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and.

205. Rafi Goldberg, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities," National Telecommunications and Information Administration, 13 May 2016, https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

206. Wolf, Polonetsky, and Finch, "A Practical Privacy Paradigm for Wearables."

207. See, for example Terry, "Protecting Patient Privacy in the Age of Big Data"; Terry, "Health Privacy is Difficult but Not Impossible in a Post-HIPAA Data-Driven World." See also Basel Kayyali, David Knott, and Steve Van Kuiken, "The Big-data Revolution in US Health Care: Accelerating Value and Innovation," McKinsey & Company, Apr. 2013, http://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-big-data-revolution-in-us-health-care; European Data Protection Supervisor, "Meeting the Challenges of Big Data. A Call for Transparency, User Control, Data Protection by Design and Accountability," 25 Nov. 2015, https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/BigDataQA; Center for Democracy and Technology, 21 Apr. 2015, "Health Big Data in the Commercial Context," https://cdt.org/insight/health-big-data-in-the-commercial-context/; Electronic Frontier Foundation, "The Law and Medical Privacy"; World Privacy Forum, "New WPF Report—The Precision Medicine Initiative and Privacy: Will Any Legal Protections Apply?" 18 May 2016, https://www.worldprivacyforum.org/2016/05/wpf-report-the-precision-medicine-initiative-what-laws-apply/.

208. Except for our brief overview of existing health regulations in the preceding section, we do not attempt to delve deeply into the details of specific laws and rules in the medical sector. Many of our colleagues in the privacy, health advocacy, patient rights, and civil liberties communities have much more expertise in these areas than we do, and they have put a great deal thought and effort into how patient and health privacy should be protected in response to the challenges presented by technological change. Our intention here is to build on this important work. The nonprofit Patient Privacy Rights organization, working with the Partnership for Patient Privacy, Microsoft, and a health consulting firm, has developed a Patient Privacy Rights Framework that includes a set of privacy principles, as well as 75 "auditable criteria" that can measure the effectiveness of privacy protection on websites, mobile apps, and electronic records systems. Patient

Citations: Main Text

Privacy Rights Foundation, "Trust Framework," https://patientprivacyrights.org/trust-framework/. See also Electronic Frontier Foundation, "Medical Privacy"; World Privacy Forum, "Health Privacy," https://www.worldprivacyforum.org/category/health-privacy/; Privacy Rights Clearinghouse, "Fact Sheet 8a: Health Privacy: HIPAA Basics," https://www.privacyrights.org/content/health-privacy-hipaa-basics; Electronic Privacy Information Center, "Medical Record Privacy"; Center for Democracy & Technology, "Health Privacy," https://cdt.org/issue/privacy-data/health-privacy/; Consumers Union, "Health Information Technology," http://consumersunion.org/topic/health-care/health-information-technology/.

209. Hurley, "Taking the Long Way Home: The Human Right of Privacy."

210. Gellman, "Fair Information Practices: A Basic History." See also Dixon, "A Brief Introduction to Fair Information Practices."

211. Organization for Economic Cooperation and Development, "OECD Privacy Principles: Individual Participation Principle," http://oecdprivacy.org/#participation.

212. Organization for Economic Cooperation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

213. Gellman, "Fair Information Practices: A Basic History"; Dixon, "A Brief Introduction to Fair Information Practices."

214. Mayer-Schönberger and Cukier, Big Data: *A Revolution that Will Transform how we Live, Work, and Think,* p. 104. See also President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective,* (Washington, DC: CreateSpace Independent Publishing Platform, 2014); The White House, "PCAST Releases Report on Big Data and Privacy," 1 May 2014, https://www.whitehouse.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy. According to Barocas and Nissenbaum, the term "Big Data" means many things, but its basic paradigm involves "a belief in the power of finely observed patterns, structures, and models drawn inductively from massive datasets." Barocas and Nissenbaum, "Big Data's End Run Around Anonymity and Consent."

215. Nicolas Terry, "Navigating the Incoherence of Big Data Reform Proposals," *Journal of Law, Medicine & Ethics* 43, n. 1 (Spring 2015): 44–47, doi:10.1111/jlme.12214; Solon Barocas and Helen Nissenbaum, "Big Data's End Run Around Anonymity and Consent," in Juliana Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, eds., *Privacy, Big Data and the Public Good: Frameworks for Engagement* (New York: Cambridge University Press, 2014), pp 44-75.

216. Principle #1 of the OECD Privacy Principles, "Collection Limitation Principle," is also used interchangeably with "data minimization." See, for example, Federal Trade Commission, "Internet of Things—Privacy & Security in a Connected World," p. iv.

217. Mayer-Schönberger and Cukier, *Big Data: A Revolution that Will Transform how we Live, Work, and Think.*

218. Mayer-Schönberger and Cukier, *Big Data: A Revolution that Will Transform how we Live, Work, and Think,* p. 104.

219. Organization for Economic Cooperation and Development, "OECD Privacy Principles: Individual Participation Principle."

220. Ira S. Rubenstein, "Big Data: A Pretty Good Privacy Solution," *Big Data and Privacy: Making Ends Meet. Big Data & Privacy: Workshop Paper Collection,* Future of Privacy Forum, Stanford Law School, and The Center for Internet and Society, Sept. 2013, pp. 106–9, https://fpf.org/wp-content/uploads/TECH-Rubinstein-Big-Data-A-Pretty-Good-Privacy-Solution.pdf.

221. Cynthia Dwork and Deirdre K. Mulligan, "It's not Privacy, and it's not Fair," 66 *Stanford Law Review Online* 35, 3 Sept. 2013, https://www.stanfordlawreview.org/online/privacy-and-big-data-its-not-privacy-and-its-not-fair/.

222. As Robert Gellman points out, while notice and choice is sometimes presented by U.S. federal agencies and industry trade associations as an implementation of the Fair Information Practices, it "clearly falls well short of FIPs standards." Gellman, "Fair Information Practices: A Basic History."

223. Solon Barocas and Helen Nissenbaum, "On Notice: The Trouble with Notice and Consent," Proceedings of the Engaging Data Forum: The First International Forum on the Application and

Citations: Main Text





Management of Personal Electronic Information, Oct. 2009, https://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf; Robert H. Sloan and Richard Warner, "Beyond Notice and Choice: Privacy, Norms, and Consent," *The Journal of High Technology Law* 14, n. 2 (July 2014): 370-414, https://www.suffolk.edu/documents/jhtl_publications/SloanWarner.pdf.

224. "Privacy Policy Analysis," KnowPrivacy, http://knowprivacy.org/policies.html.

225. See generally the research of Professors Alessandro Acquisti and Lorie Cranor at Carnegie Mellon University: Alessandro Acquisti, "Research," Heinz College, Carnegie Mellon University, http://www.heinz.cmu.edu/~acquisti/research.htm; "Privacy Decision Making, Carnegie Mellon University CyLab Usable Privacy and Security Laboratory, http://cups.cs.cmu.edu/privacy-decisions.html; The Usable Privacy Policy Project, https://usableprivacy.org/.

226. Federal Trade Commission, "Internet of Things—Privacy & Security in a Connected World."

227. See, for example, Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma," 126 *Harvard Law Review* 1880 (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

228. Solove, "Privacy Self-Management and the Consent Dilemma"; Alessandro Mantelero, "Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection," *Computer Law and Security Review* 32 (2016): 238-255, http://staff.polito.it/alessandro.mantelero/Mantelero_Personal_data_for_decsional_purposes_CLSR_2016.pdf.

229. Frank Pasquale, "Redescribing Health Privacy: The Importance of Information Policy." *Houston Journal of Health Law & Policy* 14 (2014): 95–128.

230. Organization for Economic Cooperation and Development, "OECD Privacy Principles: Openness Principle," http://oecdprivacy.org/#openness.

231. Our findings were consistent with those in a 2013 Privacy Rights Clearinghouse study, which examined 43 popular health and fitness apps (both free and paid) from both a consumer and technical perspective and found that less than half even provided a link to their privacy policies, and many of them sent unencrypted data to third-party sites without users' knowledge. "Privacy Rights Clearinghouse Releases Study: Mobile Health and Fitness Apps: What Are the Privacy Risks?" 15 July 2015, https://www.privacyrights.org/mobile-medical-apps-privacy-alert. See also Forbrukerrådet, "Health and Fitness Apps Violate Users Privacy," 25 Feb. 2016, http://www.forbrukerradet.no/side/health-and-fitness-apps-violate-users-privacy/.

232. As Helen Nissenbaum and Solon Barocas explain, for example, privacy policies designed to disclose a company's data practices in user-friendly language inevitably suffer from the "transparency paradox," resulting in explanations that obscure and oversimplify what is actually taking place. Barocas and Nissenbaum, "Big Data's End Run Around Anonymity and Consent."

233. Joseph Turow, "Obfuscation & Hidden Curriculum: Understanding the Challenge of Big Data Retailing," unpublished memo prepared for The Little Meeting on Big Data. Healthy Eating Research Program of the Robert Wood Johnson Foundation and the Center on Media and Human Development at Northwestern University, 22 June 2016.

234. Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

235. See, for example, Electronic Privacy Information Center, "Algorithmic Transparency: End Secret Profiling," https://epic.org/algorithmic-transparency/.

236. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers." For example, the Network Advertising Initiative (NAI), in its 2013 Code of Conduct, has created a list of "sensitive health data," which includes cancer, mental health-related conditions, and sexually transmitted diseases, while identifying as non-sensitive such conditions as acne, high blood pressure, and cholesterol management. Network Advertising Initiative, "The NAI Code of Conduct."

237. The following illustrations from a European Union policy paper show how a variety of seemingly innocuous information can yield detailed and rich health profiles about individuals. These could include, for example,"information such as the fact that a woman has broken her leg…is wearing glasses or contact lenses…or about a person's intellectual and emotional capacity (such as IQ), information about smoking and drinking habits, data on allergies disclosed to private entities (such as airlines) or to public bodies (such as schools); data on health conditions to be used in emergency (for example information that a child taking part in a summer camp or similar event

Citations: Main Text






suffers from asthma), membership in patient support group or Weight Watchers or alcoholics anonymous." Article 29 Working Party, "Annex—Health Data in Apps and Devices," Feb. 2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

238. Under Armour, "Under Armour Privacy Policy," https://account.underarmour.com/privacy#under-armour-privacy-policy.

239. These include "persistent identifiers" and other online tracking devices that follow an individual's movements; facial-recognition technologies that enable the identification of individuals through online photos (including those posted by friends); and "lookalike modeling." Because only a small number of people are needed to make highly accurate and predictable inferences about a much larger group, Nissenbaum and Barocas refer to this practice as the "tyranny of the minority," whereby "the volunteered information of the few can unlock the same information about the many." Barocas and Nissenbaum, "Big Data's End Run Around Anonymity and Consent." In October, the European Court of Justice decided that IP addresses were to be considered as personal information. Rick Mitchell, "IP Addresses Are Protected Personal Data, EU Top Court Rules," Bloomberg Law: Privacy & Data Security, 19 Oct. 2016, http://www.bna.com/ip-addresses-protected-n57982079024/.

240. The FTC's Internet of Things report suggested a number of best practices for the de-identification of data, including the U.S. Department of Health and Human Service regulations requiring HIPAA-covered entities either to remove certain identifiers, such as date of birth and five-digit ZIP code, from protected health information, or having an expert determine that the risk of re-identification is "very small." Federal Trade Commission, "Internet of Things—Privacy & Security in a Connected World," pp. 53-54.

241. Barocas and Nissenbaum, "Big Data's End Run Around Anonymity and Consent," p. 45.

242. The FTC staff, in its Internet of Things report, has chosen to take a "flexible approach" to data limitation, "recognizing the need to balance future, beneficial uses of data with privacy protection." The report suggests a number of options to companies: "They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data." Federal Trade Commission, "Internet of Things—Privacy & Security in a Connected World," pp. 53-54.

243. Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Redwood City, CA: Stanford Law Books, 2009); The White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy."

244. Bates, "Mobile Apps Study Underscores Necessity of Strong Best Practices for Health and Wellness Data."

245. "While often hidden, the common attributes of the group can emerge during this process and so this impact assessment process provides the opportunity to identify the stakeholders who should be involved in the assessment process as a means to give voice to those collective interests." Alessandro Mantelero, "Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection," *Computer Law & Security Review* 32, n. 2 (Apr. 2016): 238-255, https://works.bepress.com/alessandro_mantelero/7/.

246. Insights from other impact-assessment methods, for example, from environmental impact assessments, could be applied and further developed over time. For example, low-risk, routine practices would not require deeper analysis; while high-risk, novel practices with impacts difficult to assess would require deeper review approaches.

247. Federal Trade Commission, "Revised Children's Online Privacy Protection Rule Goes into Effect Today," 1 July 2013, https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect.

248. One model would be the Consumer Financial Protection Bureau (CFPB), which was established in 2010 through the Dodd-Frank Wall Street Reform and Consumer Protection Act, in response to the financial crisis that began several years before. Its jurisdiction covers a wide range of institutions in the banking and financial services industries. The White House, "Wall Street Reform: The Dodd-Frank Act," https://www.whitehouse.gov/economy/middle-class/dodd-frank-wall-street-reform; Consumer Financial Protection Bureau, http://www.consumerfinance.gov.

Citations: Main Text





249. Robert Gellman, "A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board," *Hastings Law Journal* 54 (Apr. 2003): 1183-1226, http://www.bobgellman.com/rg-docs/Gellman-Hastings-03.pdf; Electronic Privacy Information Center, "Testimony and Statement for the Record of Marc Rotenberg, President, EPIC, Adjunct Professor, Georgetown Law, Hearing on 'Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows,'" Joint Hearing Before the United States House of Representatives Energy & Commerce Subcommittees on Commerce, Manufacturing, and Trade and Communications and Technology, 3 Nov. 2015, https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf.

250. The current proceeding by the FCC to ensure consumer control over the data gathered by broadband service providers is a potential initial step in creating a more robust governmental regime for privacy. Federal Communications Commission, "FCC Releases Proposed Rules to Protect Broadband Consumer Privacy," 1 Apr. 2016, https://www.fcc.gov/es/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy.

251. Public Citizen, "FDA Must Stop Manufacturers' Off-Label Promotion of Dangerous Diabetes Medications," 31 Mar. 2015, http://www.citizen.org/pressroom/pressroomredirect.cfm?ID=5460; PharmedOut, http://www.pharmedout.org/index.html.

252. Justin Wm. Moyer, "American Medical Association Urges Ban on TV Drug Ads," *Washington Post,* 19 Nov. 2015, https://www.washingtonpost.com/news/morning-mix/wp/2015/11/19/american-medical-association-urges-ban-on-tv-drug-ads/; American Medical Association, "AMA Calls for Ban on Direct to Consumer Advertising of Prescription Drugs and Medical Devices," 17 Nov. 2015, https://www.ama-assn.org/content/ama-calls-ban-direct-consumer-advertising-prescription-drugs-and-medical-devices.

253. Food and Drug Administration, "Brief Summary and Adequate Directions for Use: Disclosing Risk Information in Consumer-Directed Print Advertisements and Promotional Labeling for Prescription Drugs, Guidance for Industry, Revised Draft Guidance," Aug. 2015, http://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm069984.pdf; David L. Riggs, Stacy M. Holdsworth, and David R. McAvoy, "Direct-to-Consumer Advertising: Developing Evidence-Based Policy to Improve Retention and Comprehension," [Supplementary Web Exclusive], *Health Affairs* (28 Apr 2005): W4-249-52, http://content.healthaffairs.org/content/early/2004/04/28/hlthaff.w4.249; Kathryn J. Aikin, Amie C. O'Donoghue, John L. Swasy, and Helen W. Sullivan, "Randomized Trial of Risk Information Formats in Direct-to-Consumer Prescription Drug Advertisements," Medical Decision Making 31 (20 June 2011): 23-33, http://www.fdanews.com/ext/resources/files/archives/m/MDM.pdf.

254. Office of the National Coordinator for Health Information Technology, "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap."

255. "Apple Announces New ResearchKit Studies for Autism, Epilepsy & Melanoma," 15 Oct. 2015, http://www.apple.com/pr/library/2015/10/15Apple-Announces-New-ResearchKit-Studies-for-Autism-Epilepsy-Melanoma.html.

256. Daniel Coughlin, "Why Researchers Are Flocking to Fitbit in the Fight Against Disease," Wareable, 17 June 2016, http://www.wareable.com/fitbit/fitbit-clinical-studies-researchers-887.

257. The White House, "Precision Medicine Initiative: Privacy and Trust Principles," 9 Nov. 2015, https://www.whitehouse.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf. In 2015, the U.S. Department of Health and Human Services (HHS) and 15 other federal departments and agencies announced proposed revisions to the regulations for protection of human subjects in research, the so-called Common Rule that has been in place since 1991. HHS published a Notice of Proposed Rulemaking (NPRM) on September 8, 2015, seeking "comment on proposals to better protect human subjects involved in research, while facilitating valuable research and reducing burden, delay, and ambiguity for investigators." U.S. Department of Health and Human Services, "Federal Policy for the Protection of Human Subjects ('Common Rule')," http://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/; U. S. Department of Health and Human Services, "HHS Announces Proposal to Update Rules Governing Research on Study Participants," 2 Sept. 2015, http://www.hhs.gov/about/news/2015/09/02/hhs-announces-proposal-to-update-rules-governing-research-on-study-participants.html; U. S. Department of Health and Human Services, "NPRM for Revisions to the Common Rule," http://www.hhs.gov/ohrp/regulations-and-policy/regulations/nprm-home/. See also Tiffany Fox, "UC San Diego Launches CORE Project to Foster Ethical Research Using Personal Health Data," UC San Diego News Center, 25 Nov. 2015, http://ucsdnews.ucsd.edu/pressrelease/uc_san_diego_launches_core_project_to_foster_ethical_research_using_persona.

Citations: Main Text

258. Brent Daniel Mittelstadt and Luciano Floridi, "The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts," *Science and Engineering Ethics* 22, n. 2 (23 May 2015): 303-341; Dwork and Mulligan, "It's not Privacy, and it's not Fair."

259. Malkia Amala Cyril, "Black America's State of Surveillance," *The Progressive,* Apr. 2015, http://www.progressive.org/news/2015/03/188074/black-americas-state-surveillance; Georgetown Law Center on Privacy and Technology, "The Color of Surveillance," 8 Apr 2016, https://www.law.georgetown.edu/academics/centers-institutes/privacy-technology/events/; The Leadership Conference, "Civil Rights Principles for the Era of Big Data," http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html.

260. Solove, "Privacy Self-Management and the Consent Dilemma"; Joseph W. Jerome, "Buying and Selling Privacy: Big Data's Different Burdens and Benefits." 66 *Stanford Law Review Online* 47, 3 Sept. 2013, http://www.datascienceassn.org/sites/default/files/Buying%20and%20Selling%20Privacy.pdf; Council of Economic Advisers, "The Digital Divide and Economic Benefits of Broadband Access," Mar. 2016, https://www.whitehouse.gov/sites/default/files/page/files/20160308_broadband_cea_issue_brief.pdf.

261. Data Justice, http://www.datajustice.org/.

262. Robert Wood Johnson Foundation, "What is a Culture of Health?" Evidence for Action, http://www.evidenceforaction.org/what-culture-health. See also Robert Wood Johnson Foundation, "From Vision to Action: A Framework and Measures to Build a Culture of Health," Fall 2015, http://www.rwjf.org/content/dam/COH/RWJ000_COH-Update_CoH_Report_1b.pdf.

Citations: Sidebars and Statistics

1. Ericsson ConsumerLab, "Wearable Technology and the Internet of Things," https://www.ericsson.com/thinkingahead/consumerlab/consumer-insights/wearable-technology-and-the-internet-of-things.

2. As Fitbit notes, "traditional watch companies such as Fossil and Movado" are playing a role as well. Fitbit, "10-K Annual Report, 2015," 29 Feb. 2016, http://d1lge852tjjqow.cloudfront.net/CIK-0001447599/e6e4d679-790f-4d27-95e3-1b98f7c7f303.html?noexit=true.

3. Warc, "Global Wearables to Double by 2020," 20 June 2016, http://www.warc.com/LatestNews/News/Global_wearables_to_double_by_2020.news?ID=3693.

4. Fitbit, "10-K Annual Report, 2015."

5. Under Armour MX, "Under Armour Future Girl," Vimeo, https://vimeo.com/66195683.

6. Under Armour, "10-K Annual Report, 2015"; Under Armour, "UA HealthBox," https://www.underarmour.com/en-us/healthbox.

7. Samsung, "Connected Care Solutions," http://www.samsung.com/us/business/by-industry/healthcare-solutions/in-health; Samsung, "Improving Home Healthcare," http://www.samsung.com/us/business/by-industry/healthcare-solutions.

8. Willa Plank and Tristan Wyatt, "The Future of the Wearables Market," *Wall Street Journal,* 13 Jan. 2016, http://www.wsj.com/articles/the-future-of-the-wearables-market-1452736738.

9. Warc, "Data, Tech, Experiences," 2016, personal copy.

10. Alyssa Zamora, "Obese Workers Cost More Than Healthcare, Absenteeism," Duke Today, 8 Oct. 2010, https://today.duke.edu/2010/10/workobese.html; Christina Farr, "How Fitbit Became the Next Big Thing in Corporate Wellness," Fast Company, 18 Apr. 2016, http://www.fastcompany.com/3058462/how-fitbit-became-the-next-big-thing-in-corporate-wellness.

11. National Institute of Diabetes and Digestive and Kidney Diseases, "Overweight and Obesity Statistics," Oct. 2012, http://www.niddk.nih.gov/health-information/health-statistics/Pages/overweight-obesity-statistics.aspx.

12. Caroline Chen and Shannon Pettypiece, "Target to Offer Fitbits to 335,000 Employees," Bloomberg Technology, 15 Sept. 2015, http://www.bloomberg.com/news/articles/2015-09-15/target-to-offer-health-tracking-fitbits-to-335-000-employees.

13. Farr, "How Fitbit Became the Next Big Thing in Corporate Wellness."

14. "Qualcomm Acquires Capsule Technologie," 14 Sept. 2014, https://www.qualcomm.com/news/releases/2015/09/14/qualcomm-acquires-capsule-technologie; Qualcomm Life, "Medical-Grade Remote Care," http://www.qualcommlife.com/mobile-medical-solutions; "Qualcomm and UnitedHealthcare Collaborate to Deliver Connected Health Solutions," 1 Mar. 2016, https://www.qualcomm.com/news/releases/2016/03/01/qualcomm-and-unitedhealthcare-collaborate-deliver-connected-health.

15. "AARP Challenges New Federal Wellness Rules Allowing Employers to Penalize Employees for Keeping Private Health Information Private," 25 Oct. 2016, http://www.aarp.org/about-aarp/press-center/info-10-2016/aarp-challenges-new-federal-wellness-rules-allowing-employers-penalize-employees-for-keeping-private-health-information-private.html; Reed Ableson, "AARP Sues U.S. Over Rules for Wellness Programs," *New York Times,* 24 Oct. 2016, http://www.nytimes.com/2016/10/25/business/employee-wellness-programs-prompt-aarp-lawsuit.html; David Certner, "New Rules on Workplace Wellness Programs Make Employees Pay for Privacy," AARP Where We Stand Blog, 10 Oct. 2016, http://blog.aarp.org/2016/10/10/new-rules-on-workplace-wellness-programs-make-employees-pay-for-privacy/.

16. U.S. Food and Drug Administration, "From the Manufacturers' Mouth to Your Ears: Direct to Consumer Advertising," http://www.fda.gov/Drugs/ResourcesForYou/SpecialFeatures/ucm319379.htm.





Citations: Sidebars and Statistics






17. The guidance also addresses product misinformation that is created by an "independent third party," such as user-generated comments. Stephanie Clifford, "F.D.A. Rules on Drug Ads Sow Confusion as Applied to Web," *New York Times,* 16 Apr. 2009, http://www.nytimes.com/2009/04/17/business/media/17adco.html?_r=3&scp=4&sq=FDA&st=cse; U.S. Food and Drug Administration, "Presentations from Public Hearing on Promotion of FDA-Regulated Medical Products Using the Internet and Social Media Tools," 12-13 Nov. 2009, http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm192703.htm.

18. According to the FDA's "Guidance for Industry" document, companies should ensure that risk information is "presented with a prominence and readability reasonably comparable to claims about drug benefits." U.S. Food and Drug Administration, "Guidance for Industry: Internet/Social Media Platforms. Internet/Social Media Platforms with Character Space Limitations—Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices," Draft Guidance, June 2014, http://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm401087.pdf. See also Thomas Abrams, "FDA Issues Draft Guidances for Industry on Social Media and Internet Communications About Medical Products: Designed with Patients in Mind," FDA Blog, 17 June 2014, http://blogs.fda.gov/fdavoice/index.php/2014/06/fda-issues-draft-guidances-for-industry-on-social-media-and-internet-communications-about-medical-products-designed-with-patients-in-mind/; U.S. Food and Drug Administration, "Office of Prescription Drug Promotion (OPDP) Research," http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm397791.htm.

19. "AMA Calls for Ban on Direct to Consumer Advertising of Prescription Drugs and Medical Devices," 17 Nov. 2015, http://www.ama-assn.org/ama/pub/news/news/2015/2015-11-17-ban-consumer-prescription-drug-advertising.page.

20. BlueKai, "Whitepaper: Data Management Platforms Demystified," http://www.bluekai.com/files/DMP_Demystified_Whitepaper_BlueKai.pdf.

21. Lotame, "1st Party Data, 2nd Party Data, 3rd Party Data: What Does It All Mean?" 10 Nov. 2013, https://www.lotame.com/resource/1st-party-2nd-party-3rd-party-data-what-does-it-all-mean/; "Data Triangulation: How Second-Party Data Will Eat The Digital World," Ad Exchanger, 25 Jan. 2016, http://adexchanger.com/data-driven-thinking/data-triangulation-how-second-party-data-will-eat-the-digital-world/.

22. BlueKai, "Whitepaper: Data Management Platforms Demystified."

23. Oracle, "Oracle Data Cloud: Data Directory," 2016, http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf; ALC, "ALC MD+," http://www.alc.com/smart-data-solutions/smart-data-assets/alc-md/.

24. Oracle, "Navigating the New Prescriber's Path," https://www.oracle.com/marketingcloud/gated-form/gated-content-overlay-content.html?elqoffer=NavigatingNewPrescribersPath-LifeSci_2015; Oracle, "Oracle Marketing Cloud for Life Sciences: Personalize Life Sciences Communications for Healthcare, Pharma, Biotech, and Medical Devices," https://www.oracle.com/marketingcloud/products/life-sciences.html.

25. Richie Etwaru, "How to Achieve Orchestrated Customer Engagement," PM360, 15 Dec. 2015, https://www.pm360online.com/how-to-achieve-orchestrated-customer-engagement/; IMS Health, "IMS One," http://www.imshealth.com/en/solution-areas/technology-and-applications/ims-one/ims-one-intelligent-cloud; IMS Health, "Orchestrated Customer Engagement: Orchestrate Every Customer Experience to Drive results. IMS Health. Sept. 2015, http://www.imshealth.com/en/solution-areas/technology-and-applications/orchestrated-customer-engagement.

26. Ryan McAskill, "Global mHealth Market to Reach $49.12B by 2020," mHealth Intelligence, 10 Mar. 2015, http://mhealthintelligence.com/news/global-mhealth-market-to-reach-42.12b-by-2020.

27. Wendy Davis, "Most People Don't Understand 'AdChoices' Icon," Media Post Daily Online Examiner Policy Blog, 26 May 2015, http://www.mediapost.com/publications/article/250688/most-people-dont-understand-adchoices-icon.html.

28. Davis, "Most People Don't Understand 'AdChoices' Icon."

29. Joseph Turow, Jennifer King, Chris Jay Hoofnatle, Amy Bleakley, and Michael Hennessy, "Americans Reject Tailored Advertising and Three Activities That Enable It," University of Pennsylvania Annenberg School of Communication, Sept. 2009, http://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers.

Citations: Sidebars and Statistics





30. Wendy Davis, "FTC To Examine Privacy Policies, AdChoices Icon," Media Post Daily Online Examiner Policy Blog, 25 May 2016, http://www.mediapost.com/publications/article/276719/ftc-to-examine-privacy-policies-adchoices-icon.html.

31. Aaron Smith, "Half of Online Americans Don't Know What a Privacy Policy Is," Pew Research Center FactTank, 4 Dec. 2014, http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/.

32. Alexis C. Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days," *The Atlantic*, 1 Mar. 2012, http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

33. Joseph Turow and Nora Draper, "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation," Annenberg School for Communications, University of Pennsylvania, https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and.

34. "Numbered 1 thorough 8 below, these principles are found in Part Two, paragraphs 7 though 14 of Annex to the Recommendation of the Council of 23rd September 1980: Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data." Organization for Economic Cooperation and Development, "OECD Privacy Principles," http://oecdprivacy.org/#principles.

35. Robert Wood Johnson Foundation, "From Vision to Action: A Framework and Measures to Build a Culture of Health," Fall 2015, p. 9, http://www.rwjf.org/content/dam/COH/RWJ000_COH-Update_CoH_Report_1b.pdf.

36. These rules are administered by the U.S. Department of Health and Human Services. U.S. Department of Health and Human Services, "Federal Policy for the Protection of Human Subjects ('Common Rule')," http://www.hhs.gov/ohrp/humansubjects/commonrule/.

37. "Personal Data for the Public Good: New Opportunities to Enrich Understanding of Individual and Population Health," final report of Health Data Exploration Project, Mar. 2014, http://www.rwjf.org/content/dam/farm/reports/reports/2014/rwjf411080.

38. Robert Wood Johnson Foundation, "Data for Health: Learning What Works," a report from the Data for Health Advisory Committee, 2 Apr. 2015, http://www.rwjf.org/en/library/research/2015/04/data-for-health-initiative.html.

39. "In addition to the Privacy and Trust Principles, PMI is taking steps to build security practices into the development of the initiative to ensure the confidentiality and integrity of all PMI data. The Security Policy Framework will draw on industry's best practices in identifying strong administrative, technical, and physical safeguards to ensure the confidentiality and integrity of all PMI cohort specimens and data, and will be reevaluated regularly to keep pace with an ever-advancing technological environment." The White House, "Precision Medicine Initiative: Privacy and Trust Principles," 9 Nov. 2015, https://www.whitehouse.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf.

40. Tiffany Fox, "UC San Diego Launches CORE Project to Foster Ethical Research Using Personal Health Data," UC San Diego News Center, 25 Nov. 2015, http://ucsdnews.ucsd.edu/pressrelease/uc_san_diego_launches_core_project_to_foster_ethical_research_using_persona.

41. Sage Bionetworks, "Participant-Centered Consent Toolkit," http://sagebase.org/pcc/participant-centered-consent-toolkit/.

42. Marianne Kolbasuk McGee, "Apple's ResearchKit: The Privacy Issues," Data Breach Today, 16 Mar. 2015, http://www.databreachtoday.com/apples-researchkit-privacy-issues-a-8018.

43. Johns Hopkins Medicine, "Johns Hopkins EpiWatch: App and Research Study: What is EpiWatch?" http://www.hopkinsmedicine.org/epiwatch#.V3Ksuq4rzz9.

44. Johns Hopkins Medicine, "Johns Hopkins EpiWatch: App and Research Study: EpiWatch Privacy Policy," http://www.hopkinsmedicine.org/epiwatch/privacy.html#.V3KuOa4rzz8.

45. Johns Hopkins Medicine, "Johns Hopkins EpiWatch: App and Research Study," http://www.hopkinsmedicine.org/epiwatch#.VqqaQse9Wb8.

46. Apple, "A Bold New Way to Look at Your Health," http://www.apple.com/lae/ios/health/.

47. John Wilbanks, "An Introduction to Health Commons," Science Commons, http://sciencecommons.org/projects/healthcommons.

APPENDIX A

Wearables, Health and Privacy: A European Perspective

Background Paper

Gloria González Fuster
gloria.gonzalez.fuster@vub.ac.be

1. INTRODUCTION

Wearable devices can be described as accessories or clothing items incorporating electronics, software or sensors that are typically connected to a network. Their popularity is rapidly increasing globally and in Europe. They can take many shapes, looking like glasses, bracelets, rings, or clip-ons; they may support a variety of metrics, for instance for the purpose of monitoring body functions or collecting lifestyle information, and may be used in different contexts, from sport and fitness or the provision of healthcare to child tracking.

Wearables enable the gathering of vast amounts of very diverse types data, and their expanding popularity triggers important issues for the protection of individuals' rights and freedoms. Especially threatened are the individual rights to privacy and to the protection of personal data and, most notably, the protection of the information concerning health, which Europe has traditionally regarded as deserving extraordinary safeguards. Tackling privacy concerns has thus been highlighted as a crucial factor to stimulate the further growth of wearable technology.[1]

This Background Paper describes key policy developments taking place in the European Union (EU) in the area of wearables and health privacy. First, it introduces the advent of wearables as an element of wider data processing practices. Second, it describes the EU legal framework on privacy and personal data protection, identifying its strengths and limitations in this environment. Third, it reviews relevant ad-hoc initiatives at EU level. Finally, it summarises the central pending questions.

2. PLACING WEARABLES IN THE IOT/BIG DATA/CLOUD CONTEXT

The on-going popularisation of wearables needs to be put in the context of the development of the Internet of Things (IoT), Big Data and cloud computing. The IoT represents a broad trend of connected everyday objects that are, by contrast, typically not designed to be worn but to be left operating on their own, such as the so-called 'smart appliances'. Big Data refers to the combination of huge volumes of diverse information with data mining techniques that often have 'predictive' ambitions. Cloud computing offers large computational power able to sustain all these

processes; it can provide storage solutions and support on the fly processing. The progressive integration of IoT, Big Data and cloud computing delineates the wider context of wearables' advent.

Devices such as smartphones or tablets, even if non-strictly 'wearables', share many features with wearable technology, triggering largely comparable challenges. They allow indeed for the use of a constantly expanding number of applications ('apps') gathering numerous types of data, which will often be a combination of data actively provided by users (such as data submitted by parents about their babies' eating or sleeping habits, self-reported calories consumption, or information about the menstrual cycle) and data automatically retrieved by the devices (for instance, about location, online activity, or contacts).

A peculiarity of wearable technology is that it most often relies on sensors that automatically gather certain types of data about body activity, such as heart rate, skin temperature, or number of steps walked. Some of these sensors have a clear health dimension, like in devices designed to monitor blood glucose levels. In many cases, however, health might not be the prime focus of the device, even if health-related information could be eventually revealed: based on the monitoring of body activity, a device may, for example, calculate the hours of somebody's sleep or evaluate its quality, information which could be linked to a health condition.

Users of wearables might be pushed to actively engage in the sharing of the data about them in social media and/or to an indefinite audience. Additionally, the numerous actors present in the field, which range from app developers, operating system and device manufacturers, app stores and diverse third parties, have frequently a great interest in accessing and further processing the collected data, as their business models are often based on data monetization. Data streams emanating from wearables and related apps are particularly attractive for the advertising, pharmaceutical, insurance and employment sectors. Medical research is also supposed to benefit from these unprecedented data flows.[2] The term 'Biomedical Big Data' (BBD) encapsulates the trend to promote the algorithmic analysis of multiple datasets - coming from wearables, IoT, clinical trails or social media- to improve medical knowledge, public health or clinical care, but also more generally the health and well-being industries. According to the wearables industry, policy makers should contribute to the development of wearables by facilitating their adoption as medical devices,[3] encouraging their institutionalisation.

All in all, these developments may nevertheless result in a high degree of opacity for users of wearable devices, paradigmatically unaware of the full spectrum of data being produced and amassed, of who is using or seeking to use the data, and for which purposes, of the ways in which the data are processed, of why they are the target of some ads or special adjustments, and of the potential consequences of these practices for their own lives (and for society in general).[4] Lack of transparency and limited awareness are as such in direct tension with general EU personal data protection principles, but also affect the possibility for users to give any meaningful consent to concrete data processing activities,[5] and to refuse the practices that go against their wishes.[6] Finally, a further specific problem is raised by the fact that in a number of cases wearables and apps collect information for an individual about somebody else - for instance, parents might be sold apps or devices to monitor their children's location and activities.

3. THE LEGAL LANDSCAPE

EU's approach to health privacy is marked by its fundamental rights obligations, as defined, most notably, by the Charter of Fundamental Rights of the EU.[7] The EU Charter is legally binding upon EU institutions and upon EU Member States insofar as they implement EU law. The text enshrines two crucial fundamental rights, the right to privacy and the right to the protection of personal data, which may only be limited under strict conditions.[8]

3.1. Fundamental rights to privacy and to personal data protection

The EU fundamental right to privacy is set out in the EU Charter's Article 7. It is a broad right, corresponding to the right to respect for private life of Article 8 of the 1950 European Convention on Human Rights (ECHR). It must be interpreted taking into account the case law of the European Court of Human Rights, according to which *'the protection of personal data, not least medical data, is of fundamental importance'* to its enjoyment.[9] The European Court of Human Rights has also stressed that *'[r]especting the confidentiality of health data is a vital principle'* in the legal systems of all parties to the ECHR, and that *'[i]t is crucial not only to respect the sense of privacy of a patient but also to preserve confidence in the medical profession and in the health services in general.'*[10]

The fundamental right to the protection of personal data, a relatively new EU right, is enshrined in Article 8 of the EU Charter.[11] It is structured around three pillars: the imposition of obligations on those who process personal data (the 'data controllers' or 'processors'), the granting of rights to the individuals whose personal data are processed (the 'data subjects') and the existence of independent supervisory agencies ('Data Protection Authorities', or DPAs) responsible for monitoring that applicable rights and obligations are duly respected. This fundamental right:

- is granted to *'everyone'*, that is, anyone whose personal data is processed by a controller or processor bound by EU law, and not just EU citizens;[12]
- applies to any processing of personal data,[13] understood as any operation involving any data relating to an identified or identifiable natural person;
- sets out that personal data must always be processed *'fairly'*, exclusively *'for specified purposes'*, and *'on the basis of the consent of the person concerned or some other legitimate basis laid down by law'*;[14]
- entitles data subjects to a *'right of access to data'* concerning them, and the *'right to have it rectified'*;[15] and
- explicitly foresees that *'[c]ompliance with these rules shall be subject to control by an independent authority.'*[16]

A high level of protection needs to be ensured not only under EU law, but also whenever personal data are transferred from the EU to a third country.[17] When data transfers take place on the grounds that the recipient provides an *'adequate level*

of protection', this requirement needs to understood as meaning that in the third country is guaranteed a level of protection *'essentially equivalent'* to EU protection.[18]

3.2. A framework in transition

The EU legal framework on privacy and personal data protection is currently primarily configured by Directive 95/46/EC[19] (the 'Data Protection Directive') and Directive 2002/58/EC[20] (the e-Privacy Directive), two instruments implemented across the EU by Member States' national laws. The former will be soon replaced with a new Regulation, whereas the second is currently under review.

3.2.1. The Data Protection Directive

Directive 95/46/EC has been described by the EU Court of Justice as directly implementing the requirements of Article 8 of the EU Charter,[21] and must be interpreted in this light. It has formally two main objectives: protecting the fundamental rights and freedoms of individuals, and ensuring the free flow of personal data among EU Member States.

The Data Protection Directive generally applies to any processing of personal data, including mere personal data collection.[22] It describes the principles to be respected whenever personal data are processed, such as fair processing, purpose specification, accuracy, proportionality, confidentiality and security of data, and establishes that data cannot be kept in a form permitting identification of data subjects for longer than necessary for the purposes of the processing. It details the grounds on which the processing of personal data can be legitimately based, such as, for instance, the consent of the data subject or the need to process the data for the performance of a task carried out in the public interest. The Directive also specifies the information to be provided to data subjects, and sets out a right of access data and to have data rectified, erased or blocked, as well as the right to object to certain data uses.

Automated individual decisions, that is, decisions producing legal effects concerning individuals or significantly affecting them and which are based solely on the automated processing of data intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability, or conduct, are also generally prohibited, even if exceptionally allowed.

The Data Protection Directive incorporates a special regime for *'special categories of data',* upon which are explicitly mentioned *'data concerning health'.* The processing of such data shall, in principle, be prohibited by Member States,[23] but exemptions are possible. The processing of data concerning health shall notably be permitted when required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, if processed *'by a health professional'* subject to the obligation of professional secrecy or by other persons subject to an equivalent obligation.[24] Processing data concerning health is also permitted when data subjects have given their explicit consent,[25] or if necessary to protect the vital interests of an individual.[26] Additional exemptions are notably possible for reasons of substantial public interest.[27]

3.2.2. The General Data Protection Regulation (GDPR)

In 2012, the European Commission published a legislative proposal designed to replace Directive 95/46/EC with a General Data Protection Regulation (GDPR).[28] The new instrument, which aims to strengthen individual rights and promote the efficiency of EU data protection rules, was adopted by the Council and the European Parliament on 27 April 2016,[29] and will be applicable from 25 May 2018. As a Regulation, the new instrument will be directly applicable across the EU, and should as such robustly contribute to the harmonisation of national laws.[30]

a) Advances

A series of GDPR provisions could have a positive effect on the reinforcement of individuals' rights in relation to health privacy and wearables. In addition to general improvements such as a clarification of the territorial scope of application of EU data protection rules (particularly necessary taking into account the multinational nature of many of the commercial actors involved), the detailing of the requirements for valid consent,[31] the introduction of 'data protection by design' and 'by default' as legal obligations,[32] or the regulation of data breaches,[33] must be mentioned:

- the definition of the category of **'data concerning health'**: regarded as a 'special category of data' the processing of which is generally prohibited,[34] 'data concerning health' are defined in the GDPR as *'personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status,'*[35] moreover, the GDPR's preamble clarifies that the notion includes any data *'which reveal information relating to the past, current or future physical or mental health status of the data subject,'* such as information collected in the for the provision of health care services; identifiers used for health purposes; information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test;[36]

- the incorporation a new **transparency principle:**[37] personal data must be processed *'in a transparent manner'*[38] but additionally the controller shall provide the relevant information to data subjects *'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'*;[39]

- children are recognised as deserving *'specific protection'*;[40] in this sense, when information society services are offered directly to children, the processing of data related to children below the age of 16 (or a lower age, but not below 13 years) shall only be lawful if authorised by the holder of parental responsibility;[41] moreover, the balancing between the legitimate interests of data controllers or third parties with the interests of the data subjects shall take into account, when appropriate, the fact that the data subject is a child;[42]





- a **'right to data portability'** is expressly recognised: this right entitles data subjects to receive from data controllers personal data concerning them in a structured and commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance;[43] as such, it can help data subjects move from one service or platform to another;

- decisions based solely on **automated processing,** including **profiling,**[44] which produces legal effects concerning them or similarly affects data subjects shall in principle **not be based on special categories of personal data,** such as data concerning health, unless the requirements for processing special categories of data are met and if suitable safeguards are in place; and

- **data protection impact assessments** will be compulsory prior to some data processing activities, in particular when is envisaged the *'processing on a large scale of special categories of data'* such as data concerning health.[45]

Even if the GDPR grants particular attention to detailing the requirements of the validity of individuals' consent to the processing of their personal data, consent is not the only ground that can render lawful the processing of personal data as such (that is, personal data not falling under the 'special category of data'). The different grounds that can render lawful the processing of personal data are listed in Art. 6 of the GDPR, and notably include, in addition to the possible consent of the individual, the fact that the *'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'*[46]

The possibility of grounding personal data processing on the legitimate interests of the controller or of a third party are in principle not less protective of the interests of data subjects than consent, as it requires not only the existence of a legitimate interest, but also a balancing exercise by the controller, taking into account the weight of such legitimate interest and the interests and fundamental rights and freedoms of the individuals whose data are to be processed. In accordance with the principle of accountability, it is the responsibility of the controller not just to carry out such balancing, but also to be able to demonstrate the balancing exercise has taken place.[47] The Preamble to the GDPR notes that the balancing shall notably take into consideration *'the reasonable expectations of data subjects based on their relationship with the controller',* and always require a *'careful assessment'.*[48]

b) Limitations and challenges

The upcoming GDPR, however, also includes some provisions that might negatively affect health privacy in the EU. Indeed, despite the recognition of 'data concerning health' as a 'special category of data' that shall in principle not be processed, the fact is that derogations allowing for their processing have seemingly expanded their reach.

In this sense, processing of 'special categories of data' shall for instance be permitted on the basis of the explicit consent of the data subject,[49] but also if

'processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or Member State law or pursuant to contract with a health professional,'[50] when the data are processed *'by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.'*[51]

Additionally, processing of such data will also be permitted if *'necessary for reasons of **public interest in the area of public health,** such as protecting against serious cross-border threats to health or **ensuring high standards of quality and safety of health care and of medicinal products or medical devices,** on the basis of Union law or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy'.*[52] The GDPR Preamble clarifies that here **'public health'** must be understood in light of Regulation (EC) No 1338/2008[53] as meaning *'all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality'.*[54] This corresponds thus to a broad understanding of 'public health', the invocation of which appears makes possible to trump the general prohibition of processing of data concerning health. Nevertheless, Member States are free to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data.[55]

Another way in which the invocation of health-related purposes might affect the level of protection of individuals is through scientific research. In this sense, the Preamble to the GDPR explicitly mentions that *'[s]cientific research purposes should also include studies conducted in the public interest in the area of **public health'**.*[56] The GDPR itself does not clarify how could be determined the scientific dimension of such studies, which are potentially expanding: private companies are indeed increasingly inclined to position themselves as active in the field of 'data sciences', in line with a wider narrative of portraying Big Data as a new form of discovering knowledge.

This is significant because, despite formally supporting the **'purpose limitation principle',** according to which personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, the GDPR establishes that further processing of personal data for archiving purposes in the public interest, or **scientific** and historical **research purposes** and statistical purposes shall in principle **not be considered incompatible** with the initial purposes of the data processing.[57] Furthermore, and despite the formal recognition of a **'storage limitation principle',** according to which personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which personal data are processed, personal data may be stored **for longer periods** insofar as the data will be processed solely for archiving purposes in the public interest, or **scientific** and historical **research** purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures.[58]

Finally, **'public health'** is explicitly mentioned as an 'important objective of general public interest' allowing EU and national laws to restrict most of the rights and obligations established by the GPDR.[59]

3.2.3. The e-Privacy Directive and its review

Directive 2002/58/EC is an instrument specifically concerned with particularising and complementing the Data Protection Directive for the electronic communications sector. As the Data Protection Directive is now to be replaced with the GDPR, the European Commission has launched the review of Directive 2002/58/EC, to bring it in line with the new instrument. A major open issue is the possible inclusion of some apps, in particular those providing for text messaging, under the scope of the future e-Privacy instrument; also on the table is the question of apps access to information on user's devices.[60] A public consultation on Directive 2002/58/EC and possible changes to the existing legal framework took place between April and July 2016; the results will feed the following steps by the European Commission, which may put forward a legislative proposal before the end 2016.

3.3. Two key distinctions

The described EU privacy and data protection legal framework is build upon two major legal distinctions. First, it distinguishes between 'personal data' and data that cannot be qualified as such. Second, it marks out 'data concerning health' as a 'special category of data' deserving special protection, raising the issue of how to delimit such notion.[61]

3.3.1. Personal / non-personal data

The EU right to the protection of personal data and its implementing laws apply generally to any processing of personal data. It is thus essential that all data relating to identified or identifiable persons effectively benefit from their protection. This encompasses data which have undergone pseudonymisation,[62] and requires taking into account that data that are not, a certain point, 'personal data', could be considered as such at another moment, in other circumstances.

In any case, the processing of data falling outside of the category of 'personal data' might also have legal implications. The right to privacy is indeed a broad right, which protects individuals generally against interferences with the respect for their private life, regardless of the manner in which such interferences take place. The use of anonymous data or aggregated statistics does not guarantee as such compliance with EU fundamental rights requirements, which might still be impacted depending on which actions or decisions are taken.

3.3.2. Data concerning health / other data

If all 'personal data' are protected under EU personal data protection laws, some types of data are regarded as deserving even stricter protection.[63] 'Data concerning

health' is one of them. The delimitation of this notion is however a complex and often contested issue, with persistent disparate legal solutions surfacing at national level.[64] The European Commission sought advice on the exact scope of the notion of data concerning health in relation to lifestyle and wellbeing apps from the Article 29 Data Protection Working Party, a consultative body bringing together representatives of all EU DPAs.

In its answer of February 2015,[65] the Article 29 Working Party observed that should be considered 'data concerning health', first, all medical data,[66] including any data generated by devices or apps used in a medical context even if not officially considered as 'medical devices'. 'Health data' should actually, according to the Working Party, be envisaged broadly and in any case also include information about a person's obesity, high or low blood pressure, hereditary or genetic predisposition, excessive alcohol consumption, tobacco consumption or drug use or any information where there is a scientifically proven or commonly perceived risk of disease in the future,[67] as well as any case where are processed personal data to identify disease risks.[68] In this sense, the Working Party argued that even seemingly innocuous, 'low impact' lifestyle data could come within the definition of 'health data' when tracked over time, in combination with other data, or transferred to other parties.[69]

According to the EDPS, 'lifestyle and well-being data' should, in general, be considered health data whenever they are processed in a medical context or where information regarding an individual's health may reasonably be inferred from the data, especially when they are processed by an application that aims to monitor the health or well-being of an individual, and this whether in a medical context or otherwise.[70] In any case, data controllers have to be deemed as best placed to assess and, if necessary, anticipate, the qualification of data as 'data concerning health'.[71]

Some commercial actors tend to assert that the data collected by the wearable devices they support are not to be regarded as 'data concerning health' and thus do need to be submitted to the related stringent requirements. It is also a common idea in the field, however, that devices allowing to track weight, physical activity or heart rate might have a positive impact on the users' health,[72] and indirectly drive decreases in healthcare costs for society.[73]

In November 2015, the Dutch DPA found an app launched by Nike to be in violation of data protection law.[74] The app collected a variety of metrics and tracked sport activities of users over long periods, allowing the company to evaluate their users condition. This being data concerning health, the Dutch DPA insisted the processing was only possible if based on the 'explicit consent' of the users, which must be based on appropriate information. Users, however, were not properly informed about Nike's data processing activities, and thus unable to provide any informed consent.

4. EU INSTITUTIONS AND MHEALTH POLICY

EU institutions have been developing an 'eHealth' (electronic Health) policy since the beginning of the 2000s in order to promote the cross-border, that is, intra-EU, provision of healthcare services. The notion of mHealth (mobile Health) surfaced in this context in reference to the promotion of medical and public health practices supported by mobile devices. In 2014, the European Commission launched a public

consultation centred on a Green Paper on Mobile Health[75] with the aim of finding ways to unlock the potential of mobile health in the EU - digital-based healthcare is indeed regarded as a major opportunity for European business.[76] One of the main findings of that consultation was the lack of trust in mHealth solutions. To tackle this problem, the European Commission decided to encourage the adoption of a Code of Conduct.

4.1. Code of Conduct on Privacy for mHealth apps

In March 2015 was thus launched the drafting of a Code of Conduct on Privacy for mHealth apps, led by the industry, with the European Commission acting as facilitator. It targets developers of mHealth apps, to whom it aims to provide easily understandable guidance on EU data protection rules. A first draft was made public in December 2015,[77] and in June 2016 the consolidated Draft Code of Conduct on privacy for mobile health apps was formally submitted for comments to the Article 29 Data Protection Working Party.[78] If the Working Party approves it, app developers would be able to sign it on a voluntary basis, thereby committing to its rules.

The Code focuses on apps processing personal data that encompasses 'data concerning health'.[79] However, it also refers, to 'lifestyle data', a category of data not recognised as such in EU data protection law (it is absent both from Directive 95/46/EC and from the GDPR), in order to argue that such 'lifestyle data' are not necessarily to be considered as 'data concerning health'. Concretely, according to the Code, that would be particularly the case when so-called 'lifestyle data' constitute *'raw data on an individual's habits and behaviour that do not inherently relate to that individual's health'.*[80]

This characterisation is particularly troubling from the perspective of EU data protection law, where the notion of 'raw data' also lacks any legal significance: data can be personal or not personal, concerning health or not concerning health, but there exists not special qualification for so-called 'raw data'. More importantly, the definition appears to imply that in order to be regarded as 'concerning health' data might need to *'inherently relate'* to an individual's health,[81] which is not a requirement stemming from Directive 95/46/EC, or the GDPR. The submitted Code of Conduct, therefore, brings in a confusing definition of 'lifestyle data' that relies on a seemingly distortive conceptualisation of 'data concerning health'.

The Code pivots around the need for app developers to obtain the explicit consent of data subjects to the processing of data concerning their health.[82] It notes the data subject's consent must be 'free', but does not describe the conditions under which such freedom could be guaranteed, or how to reconcile such 'free' consent with the apparent imperative falling on app developers to obtain it. As a matter of fact, the Code seems to suggest that the requirement of 'free' consent means that users should be informed they are free not to use the app, but that using it requires their 'free' consent to the processing of (health) data.[83] No particular consideration is given to the fact that potential users of health apps may easily be persons with actual or perceived health problems, putting them in a particular position in front of data requests.

More problematically, the Code advocates app developers could regard as 'good practice' the provision of *'granular consent',* which it presents as meaning that the

consent of data subjects can be sought *'during various stages of the use of the application'.*[84] Granular consent, in reality, has been supported by the Article 29 Working Party[85] in the understanding that it entails that data subjects are presented with independent choices for different types of data processing, allowing them to consent to some while refusing others. Spreading the requests for consent over time does not particularly favour the free choices of data subjects, but might instead weaken their position, as for later requests for 'free' consent they will have already installed the app, started using it, and possibly even shared significant amounts of data that they might not know how to recover.

The GDPR foresees that Member States, DPAs, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct *'intended to contribute to the proper application'* of the GDPR, *'taking account of the specific features of various data processing sectors and the specific needs of micro, small and medium-sized entreprises'.*[86] Such codes of conduct, if approved by a competent DPA, might be adhered by data controllers or processors not falling under the scope of the GDPR to provide appropriate safeguards within the framework of data transfers to third countries, if they make binding and enforceable commitments to apply them.[87]

4.2. EDPS initiatives

The EDPS is a DPA advising EU institutions on policies and legislation that affect privacy and personal data protection. In relation to mHealth apps and devices, the EPDS has notably stressed the importance of the data minimisation principle.[88] The EDPS also identified as a key problem the scarcity of appropriate, privacy-respectful tools and practices available for the development of mHealth devices and apps,[89] and announced work on these matters through the Internet Privacy Engineering Network (IPEN),[90] an initiative founded in 2014 to encourage cooperation between engineers and legal and regulatory experts.

The EDPS has also recently set up an Ethics Advisory Board to provide advice on future challenges related to data and technology, and declared that the Ethics Advisory Board will be supported by experts with specific knowledge in areas such as health.[91]

5. CONCLUDING REMARKS

The progressive adoption of wearables triggers critical challenges for health privacy. In EU law, this translates into specific pressure on the fundamental rights to privacy and to the protection of personal data. The recently adopted GDPR provides a series of elements that might reinforce the level of protection of individuals, but important issues remain unresolved. Three must be highlighted.

First, a key issue is making sure that all the different actors potentially involved in the (further) processing of data concerning health generated by wearable technology are effectively engaged in privacy and personal data protection compliance. Whereas providing guidance to app developers or enlarging their technological choices might be a good starting point, the fact is that the main privacy problem





of wearables are to some extent not wearables as such, but their integration in wider data ecosystems. This needs to be acknowledged and addressed, recognising the limitations of upstream mechanisms such as 'data protection by design' or 'by default' in scenarios where the major threat are downstream data practices.

Second, and although the GDPR openly concedes that children 'merit' specific protection, the EU legal framework still lacks provisions that would effectively provide such merited specific safeguards. This problem is particularly acute in the wearable field, as children might find themselves at the first line of data collection, in many occasions as the result of deliberate decisions or actions of their parents - who cannot be regarded, in these circumstances, as a reliable source to consent to, or refuse, subsequent data processing practices in their name.

Third, and finally, EU policy seems to be advancing towards a situation where would coexist a particularly narrow construction of the notion of 'data concerning health', that is, of the data formally granted special protection due to their sensitive nature, and a tendency to broaden the grounds that allow for (further) data processing activities for health-related purposes. This may give rise to undesirable gaps, as the incentives to engage in (further) health-related processing are many, whereas the cases in which the sensitive nature of health-related data represents an effective obstacle to its processing may become increasingly rare.

Most importantly, this parallel trend of simultaneously trying to narrow the scope of protection (notably putting pressure on the contours of the notion of 'data concerning health') while expanding the reach of permissible exemptions (widely supporting data processing in the name of science or health) goes against key basic principles enshrined in the case law of the EU Court of Justice, which is grounded in the fundamental rights dimension of EU personal data protection. In this sense, the Court of Justice has repeatedly emphasised that EU personal data protection law needs to be interpreted as to guarantee the *'effective and complete protection of data subjects'*,[92] which demands a broad interpretation of the notions delimiting its scope of application,[93] and a narrow circumscription of its limitations.[94]

Citations: Appendix A

1. In this sense: Fabian Nagtegaal et al. (2015), *Internet of Things: Wearable Technology,* Business Innovation Observatory, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, European Commission, February 2015, p. 2.
2. In this sense, for instance: European Data Protection Supervisor (EDPS), *Opinion 1/2015: Mobile Health - Reconciling Technological Innovation with Data Protection,* 21 May 2015, Brussels, p. 9.
3. Nagtegaal et al. (2015), op. cit., p. 2.
4. See also: Gloria González Fuster and Amandine Scherrer (2015), *'Big Data and Smart Devices and their Impact on Privacy',* under the coordination of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and the Centre for European Policy Studies (CEPS), Policy Department C – Citizens' Rights and Constitutional Affairs European Parliament.
5. Article 29 Data Protection Working Party (2013), Opinion 02/2013 on Apps on Smart Devices WP 202, 27 February 2013, Brussels, p. 5.
6. Ibid., p. 2.
7. Charter of Fundamental Rights of the European Union, OJ C83, 30/03/2010, pp. 389-410.
8. Defined in the EU Charter's final clauses, and particularly its Art. 52(1).
9. See Judgment of the ECtHR (Fourth Section) of 29 April 2014, *L.H. v Latvia,* Application no. 52019/07, para. 56.
10. Idem.
11. On this right, see: Gloria González Fuster (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer, Dordrecht.
12. Art. 8(1) of the EU Charter.
13. Idem.
14. Art. 8(2) of the EU Charter.
15. Idem.
16. Art. 8(3) of the EU Charter.
17. See notably: EUCJ, Judgment of the Court (Grand Chamber) of 6 October 2015, Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* para. 72.
18. Ibid., para. 73.
19. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23/11/1995, pp. 31-50.
20. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L201, 31.7.2002, pp. 37–47, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L337, 18.12.2009, pp. 11–36.
21. EUCJ, Judgment of the Court (Grand Chamber) of 13 May 2014, Case C 131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* para. 59.
22. Art. 2(b) of Directive 95/46/EC.

Appendix A: Citations

23. Art. 8(1) of Directive 95/46/EC.

24. Art. 8(3) of Directive 95/46/EC.

25. Unless a national law does not allow it - Art. 8(2)(a) of Directive 95/46/EC.

26. Art. 8(2)(c) of Directive 95/46/EC.

27. Art. 8(4) of Directive 95/46/EC.

28. European Commission (2012), *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),* COM(2012) 11 final, 25 January 2012, Brussels.

29. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR), OJ L119, 4.5.2016, pp. 1-88.

30. EU Member States, nevertheless, are granted the possibility to adopt national-specific rules on a series of matters, such as, for instance, the processing of national identification numbers or any other identifier of general application (Art. 87 of the GDPR).

31. Defined as *'any freely given, specific, informed and unambiguous indication'* of their wishes, given *'either by a statement or by a clear affirmative action'* (Art. 4(11) of GDPR).

32. Art. 25 of the GDPR.

33. Arts. 33 and 34 of the GDPR.

34. Art. 9(1) of the GDPR. Another category among these special categories is 'genetic data', defined as *'all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the psychology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question'* (Art. 4(13) of the GDPR).

35. Art. 4(15) of the GDPR.

36. Recital (35) of the GDPR.

37. Gloria González Fuster (2014), 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection', *IDP Revista de Internet, Derecho y Política,* N° 19, November 2014, pp. 92-104.

38. Art. 5(1)(a) of the GDPR.

39. Art. 12(1) of the GDPR.

40. Recital (38) of the GDPR.

41. Art. 8(1) of the GDPR.

42. Art. 6(1)(f) of the GDPR.

43. Art. 20 of the GDPR.

44. Defined as *'any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'* (Art. 4(4) of the GDPR).

45. Art. 35(3)(b) of the GDPR.

46. Art. 6(f) of the GDPR

Appendix A: Citations

47. Art. 5(2) of the GDPR.

48. Recital 47 of the GDPR.

49. Art. 9(2)(a) of the GDPR.

50. Art. 9(2)(h) of the GDPR.

51. Art. 9(3) of the GDPR.

52. Art. 9(2)(i) of the GDPR.

53. Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, OJ L354, 31.12.2008, pp. 70–81.

54. Recital (54) of the GDPR.

55. Art. 9(4) of the GDPR.

56. Recital (159) of the GDPR.

57. Art. 5(1)(b) of the GDPR.

58. Art. 5(1)(e) of the GDPR.

59. Art. 23(1)(e) of the GDPR.

60. See European Commission's announcement of the Stakeholder Workshop 'Towards a future proof ePrivacy legal framework'.

61. Also emphasising the relevance of these distinctions: EDPS, Opinion 1/2015, op. cit.

62. Recital (26) of the GDPR is clear in this regard. See also EDPS, Opinion 1/2015, op. cit., p. 5.

63. For the purposes of the GDPR, the processing of personal data must always be based in one of the grounds enumerated in its Art. 6(1), whereas the processing of special categories of data is only permissible if based on the grounds listed in Art. 9(2).

64. Configuring what has been described as the *'rather obscure'* area of national regulation of sensitive data processing (Douwe Korff (2010), *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments,* European Commission, 2010, p. 75).

65. Article 29 Working Party (2015), Letter from the ART 29 WP to the European Commission, DG CONNECT on mHealth and its Annex - 'Health data in apps and devices', 5 February 2015, Brussels.

66. Noting patients have a right to privacy like any other individual, Article 29 Data Protection Working Party (2007), *Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR),* WP131, 15 February 2007, p. 21.

67. Annex, p. 2.

68. Ibid., p. 3.

69. Idem.

70. EDPS, *Opinion 1/2015*, op. cit., p. 5.

71. Ibid., p. 7.

72. In this sense, for instance, Nagtegaal et al. (2015), op. cit., p. 7.

73. Ibid., p. 8.

74. Autoriteit Persoonsgegevens (2015), *Translation Press Release 10 November 2015: Nike modifies running app after Dutch DPA investigation,* 30 November 2015.

75. European Commission (2014), *Green Paper on mobile Health ('mHealth'),* COM(2014) 219 final, 10.4.2014, Brussels. It was published together with a Staff Working Document providing legal guidance on EU legislation in the field to app developers, medical device manufacturers, digital distribution platforms (European Commission (2014), *Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps,* SWD(2014) 135 final, 10.4.2014, Brussels).

76. In this sense: Andrus Ansip (2016), *Health and Lifestyle: How Digital Tech Can Improve How We Live Blog Post,* 29 January 2016.

77. *Draft Code of Conduct on Privacy for Mobile Health Applications,* December 2015.

78. *Draft Code of Conduct on Privacy for Mobile Health Applications,* June 2016.

79. Ibid., p. 2.

80. Idem.

81. Reference is also made to the need for data to have a *'clear and close link'* to a person's health status (idem).

82. Ibid., p. 6.

83. The recommended notice would *'[i]nform the user that their use of the app is strictly voluntarily, but requires their consent to permit the processing of personal data',* ibid., p. 10.

84. Ibid., p. 6.

85. Article 29 Data Protection Working Party, Opinion 02/201, op. cit., p. 27.

86. Art. 40(1) of the GDPR.

87. Art. 40(3) of the GDPR.

88. EDPS, Opinion 1/2015, op. cit., p. 10.

89. Ibid., p. 11.

90. Idem.

91. EDPS (2015), *Opinion 4/2015: Towards a New Digital Ethics: Data, Dignity and Technology,* 11 September 2015, Brussels, p. 14.

92. See for instance: *Google Spain,* already cited, para. 38.

93. See for instance: *Google Spain,* already cited, paras. 34 and 54.

94. In this sense: EUCJ, Judgment of the Court (Grand Chamber) of 8 April 2014, Joined Cases C293/12 and C594/12, *Digital Rights Ireland and Seitlinger and Others,* para. 38

APPENDIX B

Analysis of Wearable Privacy Policies

The privacy policy format has not changed much over the past decade.[1] We examined some of the leading wearable providers' privacy policies (including those of Under Armour, Fitbit, WebMD, Walgreens, Misfit, Samsung, Google, and Apple). While we did not look at the actual data flows or attempt to assess the veracity of the disclosures or otherwise gauge the impact of these described practices, we did analyze the claims made to consumers.[2]

Wearable device companies, and their affiliates, use privacy policies to reassure consumers that the data gathering is designed to benefit them. Misfit's privacy policy, for example, states that "The information we collect helps us provide you a meaningful and customized experience while using Misfit products and services.... Our goal is to help you live a healthier, more fulfilling life outside of and within your home." It then continues to list 17 different uses, among them to "develop and improve marketing and advertising for the Services and partner services...."[3] Under Armour promises that "our mission is to make all athletes better through passion, design, and the relentless pursuit of innovation."[4] Fitbit says that it "designs products and tools that track everyday health and fitness to empower and inspire users to lead healthier, more active lives."[5] Google's privacy policy, similarly, notes that "We collect information to provide better services to all of our users...."[6]

Few privacy notices described their companies' business models, including their means of revenue generation, so that an individual would be better able to understand the data-sharing agreement they are being asked to make. Fitbit, for example, claims that "We're not in the data business, we're in the fitness business."[7] Under Armour's policy doesn't reflect what it tells advertisers, to whom it boasts of its "amazing platform," "connecting millions of users on their individual journeys," and that marketers will enjoy "Unlimited reach, regardless of technology" and "Access to the world's largest user base."[8]

These policies often assure consumers that the information being collected is either obscured or does not reveal any of their personal details. "Information that is anonymous, aggregate, de-identified, or otherwise does not reveal your identity" is how Under Armour explains it. No privacy policy we looked at warns of the ease with which data are re-identified, or the power of inference and the risks to individuals and groups stemming from such data-processing techniques. But we know that data miners can make assessments about a person that go beyond the data the individual has agreed to provide. By mining data about "people like you," a range of attributes can be inferred about you that are outside any decisional regime of individual control on which these privacy policies rely.[9]

Rather than being transparent about these risks, the privacy policies we examined often embrace taking advantage of de-identified data. Misfit's privacy policy,

for example, states that "Our use and disclosure of aggregated and/or de-identified information is not subject to any restrictions under this Privacy Policy, and we may disclose it to others without limitation for any purpose."[10] WebMD confirms that non-personal information "means information that we cannot use to identify or contact you," but points out that its partnering third parties collect non-personal information about "your usage of the WebMD Web Sites, including which health topics you have viewed," and use this information to deliver advertising on WebMD and other sites. WebMD then refers the user to these third parties' own policies (e.g., Google and Facebook) for more specific privacy information.[11]

All of the privacy policies we examined (except for Google's) fail to define clearly what they consider to be "sensitive data." Most do not alert the user about the inherent risks of collecting the most intimate details of a person's bodily functions, for example; nor do they explain that this highly sensitive data, in the wrong hands, could be used to make important inferences and decisions about a user that could affect that person's employment or insurance status or otherwise limit one's life choices.

The privacy policies of two of the companies in our analysis are noteworthy for some of their positive features. Google, for example, handles "sensitive personal information" differently from other players (sharing with third parties "information relating to confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality" only with opt-in consent), and specifies "sensitive categories" ("An advertising category may be sensitive if it relates to topics such as race, religion, sexual orientation, or health"). Google also states that it does not "associate an identifier from cookies or similar technologies" with sensitive categories, and, importantly, imposes a "similar policy on" its advertisers. How users can make sense of this information (determining, for example, how narrow the definition of "confidential medical facts" might be, or what Google considers to be "health related") and how Google verifies these claims, are left unspecified.[12]

Apple has taken a corporate position on consumer privacy that departs from most other players, by adopting a strict set of practices for ensuring that users' data are kept on the mobile phone, Apple Watch, or other device, and making it impossible for outsiders to access that data. As explained in Apple's online privacy page,

> The Health app lets you keep all your health and fitness information under your control and in one place on your device. You decide which information is placed in Health and which apps can access your data through the Health app. When your phone is locked with a passcode or Touch ID, all of your health and fitness data in the Health app—other than what you've added to your Medical ID emergency card—is encrypted with your passcode. You can back up data stored in the Health app to iCloud, where it is encrypted while in transit and at rest.

Because of Apple's strong protection of consumer privacy, the Electronic Privacy Information Center (EPIC) honored Apple CEO Tim Cook last year at the organization's yearly Champion of Freedom event, where Cook declared his affirmation that "privacy is a fundamental right."[14]

Most websites we reviewed point out that they do not share personally identifiable information with third parties for marketing purposes. WebMD, for example,

states that "WebMD does not make your Personal Information available to third parties for their marketing purposes without your consent," and otherwise limits the sharing to a few exceptions. While it might appear as an important concession, it is in fact in the company's best interest (and reflects the online marketing industry's overall business model) to limit its sharing, so that it can most effectively monetize its data assets. Rather than give away its data, companies market on behalf of third parties and serve third-party ads or otherwise let third parties make use of the information without actually sharing it with them. The ultimate outcome for the user, however, is the same as if the data had been shared. In the financial services world this practice is referred to as "constructive sharing," since the result is often the equivalent to having shared the data.[15]

The policies generally explain that the data provided by the user will be supplemented by data from third-party entities. Google mentions "information we obtain about you from partners," while Apple seems less clear on this point, simply stating, "They [Apple and its affiliates] may also combine it with other information to provide and improve our products, services, content and advertising"—although the nature of that "other information" is not specified. Misfit's policy states in neutral language that it will supplement its data with third-party data sources to "improve" products and services: "We may get personal information about you from other sources. We may add this information to the information we have already collected from you in order to improve the products and services we provide."[16] Similarly, Under Armour says that "we may obtain demographic information about you from reputable third-party sources to help us improve our communication with you, give us better consumer insight into your needs and improve our business...."[17] And elsewhere Misfit states, "To combine wearable expertise with technology and design expertise from world-class partners, Misfit works with partners to build and bring you unique wearable experiences."[18] Similarly, Fitbit's privacy policy says that "We use...third-party data analytics platforms to improve the Fitbit Service in a variety of ways:..."[19] Such enhanced data are generally not candidly explained, however.

Similarly misnamed are the references to "choice" in these privacy policies. Fitbit believes "that consumers should exercise choice," and Under Armour "provide[s] you several ways to manage your privacy settings." The various levels of engagement required for an individual to exercise these "choices," however, are staggering, and it is no surprise that U.S. consumers feel overwhelmed rather than in control of exercising meaningful choice.[20] Once a rational user understands both a privacy policy and a company's data practices, and once this person has decided to engage in a particular activity in the first place, she still has to make a series of additional "choices" that often require studying other, third-party disclosures.[21] She has to set her privacy "choices" for social networking sites, for (third-party) advertising cookies, interest-based advertising, site analytics, for the use and sharing of location data, and possibly for the in-app sharing of data. And none of this is facilitated via a user-friendly interface. (Google, for example, lists seven bullets on the "transparency and choice" topic, each with individual links.)

For the most part, then, users are left to their own devices in figuring out what kind of value exchange they are about to enter into, and if they, their peers, and society at large will be better off as a result. Many consumers, enticed by convenience and promises of having their data protected, may unwittingly permanently consent to give away their highly sensitive data.

Citations: Appendix B

1. Paula J. Bruening and Mary J. Culnan, "Through a Glass Darkly: From Privacy Notices to Effective Transparency," *North Carolina Journal of Law and Technology,* forthcoming, http://ssrn.com/abstract=2654469; Alessandro Mantelero, "The Future of Consumer Data Protection in the E.U.: Re-thinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics," *Computer Law & Security Report,* Nov. 2014, doi: 10.1016/j.clsr.2014.09.004; Christopher Kuner, et al, "The Challenge of 'Big Data' for Data Protection," *International Data Privacy Law* 2, n. 2 (2012): 47-49, doi: 10.1093/idpl/ips003; Solon Barocas and Helen Nissenbaum, "Big Data's End Run Around Anonymity and Consent," in Juliana Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, eds., *Privacy, Big Data and the Public Good: Frameworks for Engagement* (New York: Cambridge University Press, 2014), pp. 44-75.

2. For a more technical analysis see Antoine Pultier, Nicolas Harrand, and Petter Bae Brandtzæg, "Privacy in Mobile Apps: Measuring Privacy Risks in Mobile Apps," report no. A27493, Norwegian Consumer Council, 2016, http://www.academia.edu/22037218/Privacy_in_Mobile_Apps_Measuring_Privacy_Risks_in_Mobile_Apps.

3. Misfit, "Privacy Policy," http://misfit.com/legal/privacy_policy accessed 6-29-2016.

4. Under Armour, "Under Armour Privacy Policy," https://account.underarmour.com/privacy#under-armour-privacy-policy.

5. Fitbit, "Privacy Policy," http://www.fitbit.com/legal/privacy-policy.

6. Google, "Welcome to the Google Privacy Policy," http://www.google.com/intl/en-US_us/policies/privacy/.

7. Fitbit, "Privacy Policy."

8. Under Armour, "Our Platform," http://advertising.underarmour.com/#platform.

9. Omer Tene, "People Like You," *Yale Journal of Law and Technology,* 28 Nov. 2015, http://yjolt.org/blog/2015/11/28/people-you.

10. Notably, Fitbit's privacy policy is the exception among the privacy policies we looked at and follows the FTC guidance to publicly commit not to try to re-identify data, and contractually prohibit downstream recipients from trying to re-identify data. It states, for example, that "When we provide this information, we perform appropriate procedures so that the data does not identify you and we contractually prohibit recipients of the data from re-identifying it back to you." Fitbit, "Privacy Policy."

11. WebMD, "WebMD Privacy Policy Summary."

12. Google, "Welcome to the Google Privacy Policy."

13. Apple, "A Bold New Way to Look at Your Health," http://www.apple.com/lae/ios/health/.

14. Matthew Panzarino, "Apple's Tim Cook Delivers Blistering Speech on Encryption, Privacy," TechCrunch, 2 June 2015, https://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/.

15. "Constructive sharing occurs when a financial institution provides criteria to an affiliate to use in marketing the financial institution's product and the affiliate uses the criteria to send marketing materials to the affiliate's own customers that meet the criteria." U.S. Federal Reserve, "Fair Credit Reporting Act Consumer Compliance Handbook: Fair Credit Reporting," p. 16, https://www.federalreserve.gov/boarddocs/supmanual/cch/fcra.pdf.

16. Misfit, "Privacy Policy."

17. Under Armour, "Under Armour Privacy Policy."

18. Misfit, "Privacy Policy."

19. Fitbit, "Privacy Policy."

20. Natasha Singer, "Sharing Data, but Not Happily," *New York Times,* 4 June 2015, http://www.nytimes.com/2015/06/05/technology/consumers-conflicted-over-data-mining-policies-report-finds.html?_r=0.

21. Joseph Turow, Michael Hennessy, and Nora Draper, "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation," Annenberg School for Communication, University of Pennsylvania, 2015, https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.










APPENDIX C

Recent Federal Privacy Initiatives

The White House recently warned that "massive data collection, processing, and retention in in the digital era" has challenged the country's approach to privacy. The administration's National Science and Technology Council's "National Privacy Research Strategy" report, in bold language, explained that

> the vast increase in the quantity of personal information that is being collected and retained, combined with the increased ability to analyze it and combine it with other information, is creating valid concerns about privacy and about the ability of entities to manage these unprecedented volumes of data responsibly. When information about people and their activities can be collected, analyzed, tracked, and repurposed in so many ways, it can lead to crime, discrimination, unauthorized and inadvertent disclosure, embarrassment and harassment, social stigma, inappropriate decisions, and other outcomes that may disadvantage them. That such possibilities exist can create a chilling effect on people's behaviors, which can be a significant harm in itself. A key challenge of this era is to assure that growing capabilities to create, capture, store, and process vast quantities of information will not damage the core values of the country.[1]

The report also acknowledged the critical role that protecting the data rights of individuals plays and the consequences for not doing so: "Privacy creates opportunities for political expression and choice. Privacy protections also provide a space for negotiation between consumers and businesses about data practices. When privacy is not protected, individuals and society suffer from harms, such as erosion of freedom, discrimination, loss of trust in institutions, or reduced innovation from self-censoring by the population."[2]

The White House report recognized that "the progress of privacy understanding and protection has not kept pace with the exponential increase in data collection, processing, and storage, and the resulting risks to privacy." It also acknowledged the "complex and dynamic ecosystem" for consumer data

> that includes the collectors, who may or may not have a relationship with the individual; data brokers, who buy, repackage, and sell collected information; analytics providers, who create systems for processing such information; and data users, who make decisions based upon the analytics. The plummeting cost of storage has allowed organizations to collect large amounts of data and save the data in long-term repositories, making such data available for unanticipated future use. Meanwhile, there is a growing array of always-on consumer devices, environmental sensors, and tracking technologies designed to collect, process, and archive information continuously, often without the individual knowing exactly what is being collected about him or her and how it will be used.[3]

The Obama administration's privacy framework "has been guided" by FIPPs, "supplemented by the concept of "respect for context." The role of context in privacy "creates a challenge for designing privacy-protecting systems because people will consider privacy from varied viewpoints, may use diverse terminologies to express their privacy concerns, perceive privacy-related harms differently, and vary their privacy requirements with circumstances." The report also recognized the limits of the "traditional notice and choice framework," explaining that

> privacy notices that are sufficiently detailed become too long for individuals to read and give meaningful consent, while notices that are phrased broadly in order to cover all anticipated future uses lack sufficient details for consent to be meaningful.... Today, there are so many organizations seeking to collect and use information that individuals realistically do not have the ability to evaluate each collection notice and associated data use.... Today, many data collectors disclose their data practices through privacy policies. Public posting of privacy policies promotes data collectors' accountability for their practices; however, privacy policies are often difficult to locate, overloaded with jargon, and ambiguous or open-ended in their meaning, rendering them confusing and even incomprehensible.... The burden on individuals to read and understand these policies is further compounded in the mobile context where, because of the small size of the device, a privacy policy may be spread out over 100 separate screens.[4]

The report also raised the issue of the rapidly emerging Internet of Things: "Looking forward, as surroundings are increasingly instrumented with sensors that continuously collect data in domains such as transportation, environmental control, or public safety, protecting privacy through existing disclosure mechanisms may be even more challenging. Better solutions are needed to support the various purposes of transparency, for consent and choice for individuals and for oversight by regulators."

Federal privacy experts and scholars also acknowledged that "A full treatment of privacy requires a consideration of ethics and philosophy, sociology and psychology, law and government, economics, and technology.... Privacy can be defined in multiple ways, depending on whether one highlights aspects such as solitude, confidentiality, the control of dissemination of personal information, the control of one's identity, or the negotiation of boundaries of personal spaces. Indeed, privacy definitions and characterizations continue to evolve and are an open research question.[5]

The White House privacy technology experts raised important concerns about the use of anonymization as an effective way to protect consumer privacy, noting that "As more information about individuals is retained and made available, data analytics can often be used to link sensitive information back to individuals, despite efforts to anonymize data. This situation creates opportunities for personal information to be misused." (It said that there are other more robust technical methods for anonymization, but they "come at a cost in the utility of data.")[6]

The role that "classifying and predictive algorithms" increasingly play as part of the growth of data collection and analysis was also raised, reflecting the White House acknowledgement of Big Data's potential to facilitate discriminatory or unfair practices. They noted that these algorithms "can create privacy issues when the information used by algorithms is inappropriate or inaccurate, when incorrect

decisions occur, when there is no reasonable means of redress, when an individual's autonomy is directly related to algorithmic scoring, or when the use of predictive algorithms chills desirable behavior or encourages other privacy harms."[7]

The Obama administration has called for more research that will "help bridge the gap between statements of principles and effective implementation in information systems." Only $80 million was spent on privacy research by the federal government in 2014, compared to the $3.9 billion spent overall for "Networking and Information Technology Research and Development." The new research strategy calls for multidisciplinary work, including on regulatory approaches to "understand how the adoption of privacy protections is advanced or impeded by policy and regulatory factors, organizational and business aspects, market competition, and economic and social incentives or disincentives. Multidisciplinary research is needed to gain insight into whether and when privacy protections are addressed best technologically or through ethics and policy, or some combination of all methods." It also calls for research that "include techniques for assessing the emergence, codification, and revision of societal practices, attitudes, and beliefs regarding privacy and harms from privacy events. Addressing these issues must involve technological, behavioral, economic, cultural, social, educational, psychological, ethical, and historical perspectives and related analyses."[8]

The 2015 report, "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap," released by the HHS's Office of the National Coordinator for Health Information Technology (ONC), also included a framework for privacy protections.[9] The country's goal is to have "a learning health system where individuals are at the center of their care; where providers have a seamless ability to securely access and use health information from different sources; where an individual's health information is not limited to what is stored in electronic health records, but includes information from many different sources (including technologies that individuals use)...and where public health agencies and researchers can rapidly learn, develop, and deliver cutting edge treatments."[10] Between 2021-2024 the U.S. should have a national and interoperable "learning health system, with the person at the center of a system that can continuously improve care, public health, and science through real-time data access." "Privacy Protections for Health Information" are addressed in the roadmap, which include the HIPAA Privacy Rule, the FIPPs-based "Nationwide Privacy and Security Framework," various other federal and state laws and private-sector approaches. The ONC explains in its roadmap that in a "learning health system" personal health information can be used without "express individual permission" (meaning consent) if it's to be used for "treatment, payment and healthcare operations" (called TPO). (ONC has a number of privacy-related initiatives and workgroups).[11]

Citations: Appendix C

1. National Science and Technology Council, "National Privacy Research Strategy," June 2016, p. 2, https://www.whitehouse.gov/sites/default/files/nprs_nstc_review_final.pdf.

2. National Science and Technology Council, "National Privacy Research Strategy," p. 8.

3. National Science and Technology Council, "National Privacy Research Strategy," p. 2.

4. National Science and Technology Council, "National Privacy Research Strategy," pp. 6, 14-15.

5. National Science and Technology Council, "National Privacy Research Strategy," p. 5.

6. National Science and Technology Council, "National Privacy Research Strategy," p. 7.

7. National Science and Technology Council, "National Privacy Research Strategy," p. 18.

8. National Science and Technology Council, "National Privacy Research Strategy," p. 11.

9. U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap," Final Version 1.0, Oct. 2015, https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf. ONC also released a related "Federal Health IT Strategic Plan: 2015-2020" in 2015. U.S. Department of Health and Human Services, "Final Federal Health IT Strategic Plan 2015-2020 Released," HHS.gov, 21Sept. 2015, http://www.hhs.gov/about/news/2015/09/21/final-federal-health-it-strategic-plan-2015-2020-released.html.

10. U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap," p. vi.

11. "Privacy and Security Workgroup," HealthIT.gov, https://www.healthit.gov/facas/FACAS/health-it-policy-committee/hitpc-workgroups/privacy-and-security-workgroup.