PENN STATE
UNIVERSITY PRESS

Health Wearables: Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment
Author(s): Kathryn Montgomery, Jeff Chester and Katharina Kopp
Source: *Journal of Information Policy*, Vol. 8 (2018), pp. 34-77
Published by: Penn State University Press
Stable URL: https://www.jstor.org/stable/10.5325/jinfopoli.8.2018.0034
Accessed: 02-10-2018 18:44 UTC

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

Penn State University Press is collaborating with JSTOR to digitize, preserve and extend access to *Journal of Information Policy*

JSTOR

HEALTH WEARABLES

Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment

Kathryn Montgomery, Jeff Chester, and Katharina Kopp

ABSTRACT

Wearable fitness devices have the potential to address some of the most challenging public health problems in the United States. But they also raise serious privacy concerns. The data they collect can be combined with personal information from other sources, raising the specter of discriminatory profiling, manipulative marketing, and data breaches. Yet, these devices fall between the cracks of a weak health privacy and a consumer protection system in the United States. This article offers key principles and critical issues that must be considered in order to develop effective privacy, equity, and consumer protections for the emerging digital health marketplace.

Keywords: Big Data, privacy, health wearables, policy

Two years ago, retail giant Target teamed up with Fitbit to encourage its 335,000 US 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 monthlong "Activity Challenge." The team that logged the highest average number of daily steps was awarded $1 million to distribute to their favorite local health and wellness nonprofit groups.[1] With obesity-related illnesses costing American businesses $73.1 billion per year in medical expenses and lost productivity, Target is only one of dozens of US companies embracing health and fitness trackers into their employee-wellness programs, offering various incentives to encourage

Kathryn Montgomery: American University
Jeff Chester: Center for Digital Democracy
Katharina Kopp: Center for Digital Democracy

[1] Chen and Pettypiece; Target.

JOURNAL OF INFORMATION POLICY, Volume 8, 2018

This work is licensed under Creative Commons Attribution CC-BY-NC-ND

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

participation.[2] The Equal Employment Opportunity Commission (EEOC) recently instituted rules that allow 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.[3]

A new generation of mobile apps, biosensor-equipped clothing, and wearable fitness devices is promising to help Americans 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."[4] 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.[5] The marketplace for health and fitness wearables is expected to grow, spurred by the continuing 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."[6] Between 2013 and 2015, for example, the use of mobile health apps doubled.[7] In 2016, 39.5 million adults were using a wearable device (with Internet connectivity) at least once a month. Young people between the ages of 18 and 34 were the heaviest users of the devices, with 30 percent of them wearable users, compared to a little more than half that number (an estimated 17.6 percent) for the whole population.[8] Health and fitness devices are also getting less expensive, making broader adoption by the public likely.[9]

If harnessed effectively, these new Internet-connected health and fitness devices could help address some of the most challenging public health problems in the United States. Wearables are already proving

[2] Zamora; Farr.

[3] AARP; Ableson; Certner.

[4] Ledger.

[5] Maddox.

[6] comScore; Nielsen; Quantified Self.

[7] Envolve. According to *Forbes* magazine, "approximately 24% of consumers currently use mobile apps to track health and wellness, 16% use wearable sensors and 29% use electronic personal health records. This trend is expected to continue as 47% of consumers would consider using wearables in the near future." Das.

[8] eMarketer, "eMarketer Slashes Growth."

[9] Gartner; Stables; eMarketer, "Fitness Bands Still."; "Future Market Insights (FMI)"; "The U.S. Consumer Wearables Market."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

to be useful tools for reducing healthcare 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. They are expected to be particularly beneficial for underserved communities and individuals with serious, chronic health problems.[10] 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.[11] "Increasingly, people are gathering data from their own bodies, tracking outcomes, and sharing information with colleagues and friends," explained 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.[12] Public health and medical researchers are using wearable cameras and other mobile tools to analyze real-world physical activity and sedentary behavior patterns among certain populations, tapping into a much wider spectrum of data than what is possible through traditional methods of sampling and recruitment.[13] Nonprofit health and research institutions are partnering with private, for-profit technology companies to develop large-scale medical research efforts.[14] Wearable devices could also play an important role in reducing health disparities, by facilitating access to medical treatment and enabling people to take more control of their own health-related behaviors.[15]

But some of the very features that make mobile and wearable devices so promising also raise serious concerns. The technological affordances of wearables make them particularly powerful tools for extensive data collection. Trackers, smartwatches, Internet-connected clothing, and

[10] Greer-Smith.

[11] 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. Eddy. 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.

[12] Frist.

[13] Doherty et al.; Jankowska et al.; Kerr et al.

[14] National Cancer Institute. See also World Privacy Forum, "Precision Medicine Initiative."

[15] The Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, "Understanding the Impact of Health IT."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

ingestibles enable sophisticated and intimate monitoring that far surpasses what has been possible in the past. For example, biosensors can routinely capture not only an individual's heart rate, body temperature, and movement, but also brain activity, moods, and emotions. These data, in turn, can be combined with personal information from other sources—including healthcare providers and drug companies—raising such potential harms as discriminatory profiling, manipulative marketing, and data breaches.[16]

Mobile health apps and fitness wearables are already being integrated into a growing digital marketing system whose core business model relies on continuous data collection and monitoring of individual online behavior patterns.[17] 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.[18] An expanding arsenal of software and analytic tools is enhancing the ability of digital media companies and their advertisers to glean valuable insights from the oceans of data they generate.[19] 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.[20] A variety of data-collection practices and targeting techniques 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

[16] Munro. 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. 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. Krebs and Duncan.

[17] See Montgomery, 631–48.

[18] 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." Tufekci.

[19] Smith.

[20] Campbell et al., 224; Murdough; Dăniasă; Leonhard. See also Turow, *The Daily You*; Couldry and Turow; Tufekci.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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.[21]

Yet mobile health apps and wearables currently fall between the cracks of an already weak and fragmented health privacy and consumer regulatory system in the United States.[22] 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, discrimination, and consumer-protection issues raised by these devices. 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 and its relationship to the broader health and technology sector. 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. In the following pages, we highlight several trends that are influencing the growth of the wearables marketplace, 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. We then describe the role that these devices are likely to play in the expanding

[21] For the Obama administration's response to the consumer privacy issue, see The White House, "Fact Sheet: Plan to Protect"; The White House, "We Can't Wait"; The White House, "PCAST Releases Report."

[22] 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." Terry, "Health Privacy is Difficult."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

digital marketing and big data ecosystem, along with some of the potential risks they could pose to individuals and the larger society. This discussion is followed by an assessment of the weaknesses and limitations of both government regulatory frameworks and self-regulatory regimes. Finally, we present 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.

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.[23] 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.[24]

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 contributes to a national discussion among consumers, health professionals, policy makers, industry, and the public at large.[25]

Big Data and the "New Health Economy"

Two interrelated trends are influencing the growing marketplace for health and fitness devices. One of these is the rise of Big Data, as advances in computer technology, artificial intelligence, digital communication networks, and sophisticated data-processing and data-analysis tools have triggered a

[23] As part of this inquiry, we convened a 1-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.

[24] This paper is based on an 18-month research project, funded by the Robert Wood Johnson Foundation, conducted in partnership with the Center for Digital Democracy, and released as a major report in December 2016. Accessed June 14, 2017. https://www.democraticmedia.org/CDD-Wearable-Devices-Big-Data-Report. The authors would like to thank Isabelle Zaugg for her research assistance in the early stages of this project.

[25] See, for example, The White House, "Consumer Data Privacy in a Networked World"; Federal Trade Commission, "Big Data."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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.[26]

Big Data is at the center of several major federal initiatives designed to promote greater health and well-being, address inefficiencies in our current medical system, lower costs, and contribute to improvements in outcomes.[27] The Affordable Care Act (ACA), which was enacted in 2010, included provisions for promoting the adoption of electronic health records by medical professionals and enabling patients to gain easier access to their own data.[28] Similarly, 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

[26] Mayer-Schönberger and Cukier, p. 6. "The Big Data Conundrum: How to Define it?"; Sicular.

[27] 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." Office of the National Coordinator for Health Information Technology, "Connecting Health and Care for the Nation." The Roadmap addresses a number of 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."

[28] "Federal Mandates for Healthcare."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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."[29] The growth of "precision medicine" is also transforming traditional approaches to healthcare, relying 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.[30]

The second important trend that is influencing the health and wearables marketplace is the infusion of investment money for technical innovation in the health and medical sector. 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," which includes wearables, biosensing consumer devices, and a range of other state-of-the-art health services and applications, all of which take advantage of the availability of personal

[29] 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 HIPAA 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." ONC, "Connecting Health and Care for the Nation." The Roadmap addresses a number of important data governance and security issues as well, such as "consistent" data semantics and formats.

[30] The White House, "Precision Medicine Initiative: Guiding Principles; Burwell and Monaco; White House Office of the Press Secretary; Kaiser; Wasserman. 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." Interlandi. For a critical analysis of the privacy implications of the Precision Medicine Initiative, see World Privacy Forum, "Precision Medicine Initiative."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

health data.[31] As a recent PricewaterhouseCoopers report explained, all of these trends have created a "New Health Economy" that 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."[32]

Wearables and Data-Driven Marketing

This "new health economy" is further eroding the boundaries between healthcare institutions and the digital commercial marketplace. The last several years have witnessed a proliferation of specialized services offering a variety of Big-Data services to marketers. For example, data management platforms (DMPs) provide marketers with "centralized control of all of their audience and campaign data."[33] 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.[34] 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."[35] IMS Health, which operates a data-management platform and cloud-computing service for health marketers, recommends that its clients gather behavioral and profile data

[31] Google Ventures (now GV), which invests in "early-stage" start-ups, has contributed 30 percent of its annual funding to health companies. See, for example, Venrock; GV; Sutton.

[32] PwC.

[33] BlueKai.

[34] Lotame; "Data Triangulation."

[35] BlueKai.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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."[36]

The advertising industry is gearing up to take advantage of wearables and other digital devices as key tools for data-driven targeted marketing within an increasingly seamless medical, consumer, and health ecosystem.[37] 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.[38] According to a recent survey conducted for a leading digital e-commerce marketing firm, the "key benefit 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. Smartwatches 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.[39] 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."[40]

Wearables are expected to play a major role in dramatically increasing the availability of behavioral data on individual consumers.[41] For example, 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).[42] 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

[36] Etwaru; IMS Health, "Orchestrated Customer Engagement."; IMS Health, "IMS One."

[37] TapSense.

[38] "Partner Forum"; "Innovation in a Patient-Centric World."

[39] Criteo; Martin.

[40] Gupta.

[41] "Transformational Technology."; IMS Health, "Nexxus Commercial Application Suite"; IMS Health, "Nexxus Marketing"; IMS Health, "IMS One."

[42] Under Armour, "Our Platform"; Under Armour, "MapMyFitness"; Under Armour, "Mobile Interstitials"; Under Armour, "Our Products."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

alongside smartphones, tablets, connected TVs, medical appliances, connected cars, and the "multiple embedded touchpoints" increasingly found in homes and communities.[43]

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 United States and New Zealand are the only two developed countries that permit direct-to-consumer (DTC) advertising of pharmaceutical products.[44] Though pharmaceutical marketing is federally regulated, weaknesses and loopholes in the law have enabled the industry to engage in robust advertising and promotion efforts.[45] 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 US healthcare 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

[43] Criteo.

[44] For example, the FDA U. S. Food and Drug Administration, "Keeping Watch Over Direct-to-Consumer Ads." 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. Electronic Privacy Information Center.

[45] 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. Gaffney; "Strategic Pharma Solutions. 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. See Electronic Privacy Information Center, "Medical Record Privacy."

[46] Staton.

[47] Ventola.

[48] eMarketer, "Health & Pharma Marketers."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

spending will reach $3.10 billion.[49] 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."[50] 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.[51]

The merger of connected health and digital marketing has created a new generation of data collection and digital marketing practices that are

[49] Orsini; Snider.

[50] "How Can Pharma Firms Market."

[51] "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. 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.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

currently in use by health and pharmaceutical marketers and are being developed for use in the wearables market.

"Scoring," "Personas," and "Look-alike 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."[52] Through *look-alike 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.[53] Health and pharmaceutical marketers often use look-alike 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.[54]

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

[52] Chertudi; Moked.

[53] LiveRamp. 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." Baker. See also Krux; Ransbotham.

[54] Skyhook.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

and *script targeting* services (based on analyses of prescription drug sales), where marketers can reach "patients by treatment and diagnosis."[55] 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.[56] 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 20 Google searches involves health. Nearly 50 percent of consumers search for reviews and other information on physicians.[57] African Americans and Latinos are more likely than whites to use their mobile phones to search for health information.[58]

Programmatic Marketing

Automated forms of ad buying and placement on digital media use algorithmic processes to find and target customers wherever they go. 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.[59] 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

[55] Adprime also offers services to target via mobile and video platforms. Adprime Media, "Targeting"; Adprime Media, "The Premier Ad Network."

[56] AdRx, "Advertising Partnerships"; AdRx, "Solutions." AdRx also cites its membership in self-regulatory trade organizations, including the Digital Advertising Alliance (DAA) and Network Advertising Initiative (NAI), that it is "committed to brand safety" (but doesn't mention privacy). (AdRx's website has been absorbed into that of its parent company, Conversant, and the pages referenced earlier are no longer available.)

[57] Gandhi and Wang; "How Can Pharma Firms Market."

[58] Anderson, "Racial and Ethnic."

[59] Allen.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

of a mobile device's identifiers.[60] 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.

Geolocation and Geomedical Targeting

Mobile devices continually send signals that enable advertisers (and others) to take advantage of an individual's location—through the phone's global positioning system (GPS), 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.[61] Through a host of new location-targeting technologies, consumers can now be identified continuously—while driving a car, pulling into a mall, or shopping in a store.[62] Google and Facebook, which often know the actual ("authenticated") identity of their consumers, have expanded their use of location for ad targeting.[63] In the pharmaceutical and health sector, specifically, "geomedical 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. [64] For example, one geomedical 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.[65]

[60] Xaxis, "A GeoMarketing Conversation"; Xaxis, "Xaxis Launches Light Reaction."

[61] Ryan.

[62] 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." Son et al.; "The Difference Engine."

[63] Google, "Understanding Advanced"; Facebook, "Helping Local Businesses"; Facebook, "Ad Targeting Options."

[64] Lewis.

[65] eHealthcare Solutions; 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; McCaffrey.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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.[66] 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.[67] The leading US pharmacy chains have also 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.[68] For example, 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. Consumers can also use the "symptom checker" to research conditions and medications.[69]

"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. Among these are "wearable ads" on smartwatches, which the industry sees as a particularly promising source of new revenue. 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

[66] O'Dea.

[67] Shelfbucks. For example, General Mills, Coca-Cola, Pepsi, Kellogg's, and Nestle are clients of this top and reward shopper marketing company. TPG Rewards; WireSpring Technologies; Karolefski.

[68] "Drugstores and Pharmacies."

[69] The company lists 22 apps and 36 devices that can be connected with its Balance Rewards program. Walgreens.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

matter what they are doing."[70] "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 . . . ."[71]

Toward a Fully Integrated Digital Consumer-Health Marketplace

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.[72] 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."[73] 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."[74] 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.

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 coexisting but also communicating with each other on a regular basis.[75] With consumer health and wellness data continually

[70] Baysinger.

[71] Adante.

[72] Topol; Pentland et al.

[73] Estrin and Juels.

[74] UC Berkeley Center for Long-Term Cybersecurity.

[75] Champagne et al.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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.

The same tools that people use to track their activities and monitor their bodily functions will also serve as highly personalized commercial targeting systems, delivering emotional appeals tailored to each individual's 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 smartwatch 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 farfetched 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*.[76]

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.[77]

[76] "Minority Report—Personal Advertising in the Future."

[77] Upturn; National Science and Technology Council.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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.[78] 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.[79]

Gaps and Weaknesses in Health and Privacy Regulation

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. However, none of these systems, in their current state, provides adequate safeguards to patients or consumers in the Big-Data era.

Privacy laws governing health information are limited and fragmented, with significant gaps in coverage.[80] For example, the primary purpose of the Health Insurance Portability and Accountability Act (HIPAA) is to ensure the flow of information throughout the healthcare system. More appropriately labeled a "confidentiality rule," it does little to put limits on the aggregation and analysis of health-related data.[81] 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."[82] As

[78] Electronic Frontier Foundation.

[79] See Jerome, 47–53.

[80] Peel, 89–116; Electronic Frontier Foundation. 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 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. Meingast et al.; Anderson; "How the HITECH Act Changes HIPAA Compliance."

[81] Terry, "Protecting Patient Privacy."

[82] Sweeney.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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."[83] 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.[84] Health wearables, mobile apps, fitness trackers, smartwatches, 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.)[85]

This gap in coverage was underscored in a July 2016 report by the Department of HHS, 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 "smartphones and other mobile devices," but also "peer health communities, online health management tools, and websites used to generate information for research." Many of these "noncovered 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.[86]

Nor is the Food and Drug Administration (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. Last year the FDA concluded a proceeding that considered whether

[83] Terry, "Big Data Proxies."

[84] Terry, "Protecting Patient Privacy."

[85] 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. Lee.

[86] U.S. Department of Health and Human Services.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

it should regulate health and wellness wearables.[87] The agency 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."[88] 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.

The Federal Trade Commission (FTC) is a key government agency with responsibility to protect consumer privacy online. The 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.[89] 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.[90] While the FTC has made some progress in its ongoing efforts to address the challenges of the Big-Data era, with its narrow jurisdiction, lack of rulemaking ability, and limited regulatory resources, it remains 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 sector, but also in the larger digital marketplace.

[87] 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." Lecher.

[88] U.S. Food and Drug Administration, "Webinar— Final Guidance."

[89] Turow, "Americans and Online Privacy."

[90] Spinelli; Balto.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

In the current US political environment, there are very few prospects for stronger regulations to address the Big Data, digital marketing, and health privacy issues raised by mobile apps and wearable devices, and the scattered protections in place now may well be in serious jeopardy. Moreover, in the wake of the recent presidential election, the White House has taken a particularly aggressive approach to rolling back regulations that were put in place during the previous administration. For example, in 2016 the Federal Communications Commission (FCC), which has primary jurisdiction over broadband Internet access service companies—the phone and cable companies that supply the majority of high-speed Internet connections—issued privacy rules for Internet service providers (ISPs) that classify important categories of information as "sensitive," including mobile apps, search engines, and health data, requiring prior consent (opt-in) before these data could be gathered for commercial purposes.[91] However, in February 2017, Congress passed a law that eliminated these new rules before they took effect.[92]

In the absence of a strong regulatory framework, consumers have been forced to rely on industry 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.

[91] Federal Communications Commission, "FCC Adopts Broadband Consumer Privacy Rules."

[92] Lohr.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

While some of the 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.[93] Though both the major digital advertising trade groups, Digital Advertising Alliance (DAA) and Network Advertising Initiative (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. 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 (e.g., including whether it uses sponsored content from health companies) to be able to exercise an informed decision under the DAA process.[94]

Most of the industry guidelines, moreover, 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, look-alike 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.[95]

Developing Twenty-First-Century Big-Data Safeguards

In the wake of the recent election, the United States is enmeshed in a major public debate over the future of its healthcare system. The ACA is very likely to undergo significant transformation, with millions of

[93] Digital Advertising Alliance; Davis, "NAI Issues Privacy Guidelines"; Davis, "BBB Warns Publishers."

[94] Davis, "Aetna and Sega Violated"; Advertising Self-Regulation Council.

[95] Gellman and Dixon; Hoofnagle; Center for Digital Democracy, "U.S. Online Data Trade Groups."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

Americans facing the prospect of losing their health insurance or having their coverage severely cut. Depending on the outcome of the current policy process, personal digital devices may play an important role in efforts to reduce healthcare spending. However, as this article 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.

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 suggests otherwise. 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."[96] These public sentiments are echoed in a report released by the US 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."[97]

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 that people engage with medical practitioners, employers, hospitals, and other institutions. Even as their interactions with these digital tools become normalized and routine, individuals 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.

[96] Turow and Draper.

[97] Goldberg.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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.[98] Because regulation is so fragmented and insufficient, there is an urgent need for a much broader policy framework to protect health privacy. Many experts 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.[99] But it is impossible 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, equity, and consumer protections for the emerging digital health marketplace:

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.[100] While personal health information should clearly be

[98] 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 Privacy Rights Foundation. See also Electronic Frontier Foundation; World Privacy Forum, "Health Privacy"; Privacy Rights Clearinghouse, "Fact Sheet 8a"; Electronic Privacy Information Center, "Medical Record Privacy"; Center for Democracy & Technology, "Health Privacy"; Consumers Union.

[99] 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 Kayyali et al.; European Data Protection Supervisor; Center for Democracy & Technology, "Health Big Data"; Electronic Frontier Foundation; World Privacy Forum, "New WPF Report."

[100] Federal Trade Commission, "Protecting Consumer Privacy." 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 nonsensitive such conditions as acne, high blood pressure, and cholesterol management. Network Advertising Initiative, "The NAI Code of Conduct."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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.[101] 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 the 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. 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, e-mail address,

[101] 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 suffers from asthma), membership in patient support group or Weight Watchers or alcoholics anonymous.” Article 29 Working Party.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

or other traditional identifying information.[102] De-identification and anonymization, though endorsed by regulators, are only partial solutions.[103] As scholars Solon Barocas and Helen Nissenbaum have explained, "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.'"[104]

Meaningful Transparency

Effective transparency is consistent with longstanding privacy principles.[105] 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.[106] 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

[102] 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." In October, the European Court of Justice decided that IP addresses were to be considered as personal information. Mitchell.

[103] The FTC's Internet of Things report suggested a number of best practices for the de-identification of data, including the US 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, 53–54.

[104] Barocas and Nissenbaum, "Big Data's End Run," 45.

[105] Organization for Economic Cooperation and Development.

[106] 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. See also "Privacy Rights Clearinghouse Releases Study". See also Forbrukerrådet.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

government—has triggered rising concern about how these "black box" operations can negatively impact individuals, communities, and groups.[107] To address this problem, leading public interest organizations and scholars are calling for "algorithmic transparency."[108]

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, and, if agreeing to the transaction, accept the terms of the data-processing arrangement.[109] 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.[110] Even if disclosures could be simplified, there are so many occasions for individuals to provide consent that it is practically impossible for anyone to handle the deluge of decision points.[111]

Such expectations of "privacy self-management" are at odds with contemporary Big-Data practices.[112] 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

[107] Pasquale, *The Black Box Society*.

[108] See, for example, Electronic Privacy Information Center.

[109] As Robert Gellman points out, while notice and choice is sometimes presented by US 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."

[110] Barocas and Nissenbaum, "On Notice: The Trouble with Notice and Consent"; Sloan and Warner, 370–414.

[111] See, for example, Solove, 1880–903.

[112] Solove; Mantelero, 238–55.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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."[113]

Assessing Benefits and Risks of Data Uses

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.[114] 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.[115] 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 in an accessible, consumer-friendly format comparable to nutrition labels and illuminating how certain uses of personal health data, while offering a number of benefits, might also create additional risks to individuals or groups.

Regulating Digital Pharmaceutical and Health Marketing

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

[113] Pasquale, "Redescribing Health Privacy," 95–128.

[114] "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." Mantelero.

[115] 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; whereas high-risk, novel practices with impacts difficult to assess would require deeper review approaches.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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 look-alike 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. 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. 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 other players in the health and medical industry. Today's digital practices have outpaced federal safeguards, demanding much more proactive research on contemporary market trends, closer scrutiny of emerging practices, and effective rules for addressing a range of problematic techniques. Of particular concern are techniques that enable discrimination on the basis of data related to ethnicity, gender, sexual orientation, age, community, or medical condition.

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 new 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.[116] A growing movement is underway among civil rights organizations and others to prevent the growth of a new generation of discriminatory practices.[117] We also need to ensure that programs for providing access to health technology for low-income groups

[116] Mittelstadt and Floridi, 303–41; Dwork and Mulligan.

[117] Cyril; Georgetown Law Center on Privacy and Technology; The Leadership Conference.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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.[118]

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."[119] 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 also be encouraged to inform their constituencies and the public at large about the issues raised by 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.

[118] Solove; Jerome.

[119] Data Justice.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

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. Because this market is in a fluid stage of innovation and growth, it is urgent to institute clear policies that will guarantee that the benefits to individuals and the larger society are maximized while the risks are minimized. Finally, 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."[120]

BIBLIOGRAPHY

AARP. "AARP Challenges New Federal Wellness Rules Allowing Employers to Penalize Employees for Keeping Private Health Information Private." October 25, 2016. Accessed June 13, 2017. 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.

Ableson, Reed. "AARP Sues U.S. Over Rules for Wellness Programs." *New York Times*, October 24, 2016. Accessed June 13, 2017. http://www.nytimes.com/2016/10/25/business/employee-wellness-programs-prompt-aarp-lawsuit.html.

Adante, Frank. "Wearables Usher in the Next Evolution of Consumer Engagement." Inc., April 24, 2015. Accessed June 18, 2017. http://www.inc.com/frank-addante/wearables-usher-in-next-evolution-of-consumer-engagement.html.

Adprime Media. "The Premier Ad Network." Accessed June 16, 2017. http://www.adprimemedia.com/advertisers/network_highlights.html.

———. "Targeting." Accessed June 16, 2017. http://www.adprimemedia.com/advertisers/targeting.html.

[120] Robert Wood Johnson Foundation, "What is a Culture of Health?" See also Robert Wood Johnson Foundation, "From Vision to Action."

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

AdRx. "Advertising Partnerships." Accessed May 1, 2017. http://www.adrxmedia.com/advertisers. [AdRx's website has been absorbed into that of its parent company, Conversant, and this page is no longer available online.]

———. "Solutions." Accessed May 1, 2017. http://www.adrxmedia.com/solutions. [AdRx's website has been absorbed into that of its parent company, Conversant, and this page is no longer available online.]

Advertising Self-Regulation Council. "Accountability Program Decisions, Dispositions, Closures, and Guidance." Accessed June 19, 2017. http://www.asrcreviews.org/accountability-program-decisions/.

ALC. "ALC MD+." Accessed January 15, 2018. http://www.alc.com/smart-data-solutions/smart-data-assets/alc-md/.

Allen, Robert. "What is Programmatic Marketing?" *Smart Insights*, February 8, 2016. Accessed June 18, 2017. http://www.smartinsights.com/internet-advertising/internet-advertising-targeting/what-is-programmatic-marketing/.

Anderson, Howard. "The Essential Guide to the HITECH Act." *Information Security Media Group*, February 8, 2010. Accessed June 19, 2017. http://www.healthcareinfosecurity.com/essential-guide-to-hitech-act-a-2053/op-1.

Anderson, Monica. "Racial and Ethnic Differences in How People Use Mobile Technology." *Pew Research Center FactTank*, April 30, 2015. Accessed June 18, 2017. http://www.pewresearch.org/fact-tank/2015/04/30/racial-and-ethnic-differences-in-how-people-use-mobile-technology/.

Article 29 Working Party. "Annex—Health Data in Apps and Devices." February 2015. Accessed June 20, 2017. 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.

Baker, Dillon. "How to Use Facebook's Best Feature: Targeting." Accessed June 16, 2017. https://contently.com/strategist/2015/12/16/how-to-use-facebooks-best-feature-targeting/.

Balto, David A. "Bring the FTC into the 21st Century." *The Hill*, May 4, 2010. Accessed June 19, 2017. http://thehill.com/opinion/op-ed/95947-bring-the-ftc-into-the-21st-century.

Barocas, Solon, and Helen Nissenbaum. "Big Data's End Run Around Anonymity and Consent." In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Edited by Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum, 44–75. Cambridge: Cambridge University Press, 2014.

———. "On Notice: The Trouble with Notice and Consent." *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*. October 2009. Accessed June 21, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567409.

Baysinger, Tim. "Why This Broadcaster Is Going Beyond TV to Wearables and VR." *Adweek*, August 20, 2015. Accessed June 18, 2017. http://www.adweek.com/news/television/why-broadcaster-going-beyond-tv-wearables-and-vr-166482.

"The Big Data Conundrum: How to Define it?" *MIT Technology Review*, October 3, 2013. Accessed June 14, 2017. http://www.technologyreview.com/view/519851/the-big-data-conundrum-how-to-define-it/.

BlueKai. "Whitepaper: Data Management Platforms Demystified." Accessed June 14, 2017. http://www.bluekai.com/files/DMP_Demystified_Whitepaper_BlueKai.pdf.

Burwell, Sylvia Mathews, and Lisa O. Monaco. "Precision Medicine Initiative and Data Security." *White House Blog*, May 25, 2015. Accessed June 14, 2017. https://www.whitehouse.gov/blog/2016/05/25/precision-medicine-initiative-and-data-security.

Campbell, Colin L., Leyland F. Pitt, Michael M. Parent, and Pierre R. Berthon. "Tracking Back-Talk in Consumer-Generated Advertising—An Analysis of Two Interpretative Approaches." *Journal of Advertising Research* 51, no. 1 (2011): 224–38.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

Center for Democracy & Technology. "Health Big Data in the Commercial Context." April 21, 2015. Accessed June 20, 2017. https://cdt.org/insight/health-big-data-in-the-commercial-context/.

———. "Health Privacy." Accessed June 19, 2017. https://cdt.org/issue/privacy-data/health-privacy.

Center for Digital Democracy. "New Report: Health Wearable Devices Pose New Consumer and Privacy Risks." December 15, 2016. Accessed June 14, 2017. https://www.democraticmedia.org/CDD-Wearable-Devices-Big-Data-Report.

———. "U.S. Online Data Trade Groups Spin Digital Fairy Tale to USTR about US Consumer Privacy Prowess—CDD Says Privacy Out of Bounds in TTIP." May 29, 2013. Accessed June 19, 2017. https://www.democraticmedia.org/content/us-online-data-trade-groups-spin-digital-fairy-tale-ustr-about-us-consumer-privacy-prowess.

Certner, David. "New Rules on Workplace Wellness Programs Make Employees Pay for Privacy." *AARP Where We Stand Blog*, October 10, 2016. Accessed June 13, 2017. http://blog.aarp.org/2016/10/10/new-rules-on-workplace-wellness-programs-make-employees-pay-for-privacy/.

Champagne, David, Amy Hung, and Olivier Leclerc. "How Pharma Can Win in a Digital World." *McKinsey & Company*, December 2015. Accessed June 18, 2017. http://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/how-pharma-can-win-in-a-digital-world.

Chen, Caroline, and Shannon Pettypiece. "Target to Offer Fitbits to 335,000 Employees." *Bloomberg Technology*, September 15, 2015. Accessed June 13, 2017. http://www.bloomberg.com/news/articles/2015-09-15/target-to-offer-health-tracking-fitbits-to-335-000-employees (subscription required).

Chertudi, Mikel. "Strategic Marketing Plan Element #5: The Power of Personas." *Adobe Digital Marketing Blog*, October 6, 2014. Accessed June 16, 2017. https://blogs.adobe.com/digitalmarketing/digital-marketing/strategic-marketing-plan-element-5-power-personas/.

comScore. "comScore Reports February 2016 U.S. Smartphone Subscriber Market Share." April 6, 2016. Accessed June 13, 2017. https://www.comscore.com/Insights/Rankings/comScore-Reports-February-2016-US-Smartphone-Subscriber-Market-Share.

Consumers Union. "Health Information Technology." Accessed June 19, 2017. http://consumersunion.org/topic/health-care/health-information-technology/.

Couldry, Nick, and Joseph Turow. "Advertising, Big Data, and the Clearance of the Public Realm." *International Journal of Communication* 8 (2014): 1710–726.

Council of Economic Advisers. "The Digital Divide and Economic Benefits of Broadband Access." March 2016. Accessed June 20, 2017. https://obamawhitehouse.archives.gov/sites/default/files/page/files/20160308_broadband_cea_issue_brief.pdf.

Criteo. "Ovum Report: Future of E-commerce—The Road to 2026." Accessed June 15, 2017. http://www.criteo.com/media/4094/ovum-the-future-of-e-commerce-the-road-to-2026.pdf.

Cyril, Malkia Amala. "Black America's State of Surveillance." *The Progressive*, April 2015. Accessed June 20, 2017. http://www.progressive.org/news/2015/03/188074/black-americas-state-surveillance.

Dăniasă, C. "The Mechanisms of the Influence of Viral Marketing in Social Media." *Economics, Management & Financial Markets* 5, n. 3 (September 2010): 278–82.

Das, Reenita. "Top 10 Healthcare Predictions For 2016." *Forbes*, December 10, 2015. Accessed June 13, 2017. http://www.forbes.com/sites/reenitadas/2015/12/10/top-10-healthcare-predictions-for-2016/.

Data Justice. "Challenging Rising Exploitation and Economic Inequality from Big Data," Accessed June 20, 2017. http://www.datajustice.org/.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

"Data Triangulation: How Second-Party Data Will Eat the Digital World." *Ad Exchanger*, January 25, 2016. Accessed June 19, 2017. http://adexchanger.com/data-driven-thinking/data-triangulation-how-second-party-data-will-eat-the-digital-world/.

Davis, Wendy. "Aetna and Sega Violated Industry's Mobile Privacy Code, Watchdog Says," *Media Post Daily Online Examiner*, July 14, 2016. Accessed June 19, 2017. http://www.mediapost.com/publications/article/280330/.

———. "BBB Warns Publishers To Comply With Privacy Rules." *Media Post Daily Online Examiner*, October 19, 2013. Accessed June 19, 2017. http://www.mediapost.com/publications/article/211260/bbb-warns-publishers-to-comply-with-privacy-rules.html.

———. "NAI Issues Privacy Guidelines For Digital Fingerprinting, Other Non-Cookie Ad Technology." *Media Post Daily Online Examiner*, May 19, 2015. Accessed June 19, 2017. http://www.mediapost.com/publications/article/250297/nai-issues-privacy-guidelines-for-digital-fingerpr.html.

"The Difference Engine: The Spy in Your Pocket." *The Economist*, April 29, 2011. Accessed June 18, 2017. http://www.economist.com/blogs/babbage/2011/04/mobile_tracking.

Digital Advertising Alliance. "DAA Self-Regulatory Principles." Accessed June 19, 2017. http://digitaladvertisingalliance.org/principles.

Doherty, A. R., 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 (February 13, 2013). Accessed June 13, 2017. http://www.ncbi.nlm.nih.gov/pubmed/23406270.

"Drugstores and Pharmacies." *Mobile Commerce Daily*. Accessed May 2, 2017. http://www.mobilecommercedaily.com/category/drugstores-pharmacies.

Dwork, Cynthia, and Diedra K. Mulligan. "It's not Privacy, and it's not Fair." *SLR*, September 2013. Accessed June 20, 2017. https://www.stanfordlawreview.org/online/privacy-and-big-data-its-not-privacy-and-its-not-fair/.

Eddy, Nathan. "Adoption of Health Apps, Wearable Devices Grows." *eWeek*, March 5, 2016. Accessed June 13, 2017. http://www.eweek.com/small-business/adoption-of-health-apps-wearable-devices-grows.html.

eHealthcare Solutions. "Ad Specifications." Accessed June 18, 2017. http://www.ehealthcaresolutions.com/advertisers/media-buyers/ad-specifications/#advertisers.

Electronic Frontier Foundation. "The Law and Medical Privacy." Accessed June 19, 2017. https://www.eff.org/issues/law-and-medical-privacy.

Electronic Privacy Information Center. "Algorithmic Transparency: End Secret Profiling." Accessed June 20, 2017. https://epic.org/algorithmic-transparency/.

eMarketer. "eMarketer Slashes Growth Outlook for Wearables." December 20, 2016. Accessed June 13, 2017. https://www.emarketer.com/Article/eMarketer-Slashes-Growth-Outlook-Wearables/1014896.

———. "Fitness Bands Still the Top Wearable in the U.S." May 27, 2016. Accessed June 13, 2017. http://www.emarketer.com/Article/Fitness-Bands-Still-Top-Wearable-US/1014015.

———. "Health & Pharma Marketers Split Digital Spend Between Search, Display." June 23, 2016. Accessed June 16, 2017. http://www.emarketer.com/Article/Health-Pharma-Marketers-Split-Digital-Spend-Between-Search-Display/1014123.

Envolve. "16 Care Management Predictions 2016." Author's personal copy.

Estrin, Deborah, and Ari Juels. "Reassembling Our Digital Selves." *Daedelus* 145, no. 1 (Winter 2016): 43–53.

Etwaru, Richie. "How to Achieve Orchestrated Customer Engagement." *PM360*, December 15, 2015. Accessed June 15, 2017. https://www.pm360online.com/how-to-achieve-orchestrated-customer-engagement/.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

European Data Protection Supervisor. “Meeting the Challenges of Big Data. A Call for Transparency, User Control, Data Protection by Design and Accountability.” November 25, 2015. Accessed June 20, 2017. https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/BigDataQA.

Facebook. “Ad Targeting Options.” Facebook for Business. Accessed June 18, 2017. https://www.facebook.com/business/help/433385333434831.

———. “Helping Local Businesses Reach More Customers.” *Facebook for Business*, October 7, 2014. Accessed June 18, 2017. https://www.facebook.com/business/news/facebook-local-awareness.

Farr, Christina. “How Fitbit Became the Next Big Thing in Corporate Wellness.” *Fast Company*, April 18, 2016. Accessed June 13, 2017. http://www.fastcompany.com/3058462/how-fitbit-became-the-next-big-thing-in-corporate-wellness.

“Federal Mandates for Healthcare: Digital Record-Keeping Requirements for Public and Private Healthcare Providers.” *USF Health*, June 20, 2016. Accessed June 14, 2017. http://www.usfhealthonline.com/resources/healthcare/electronic-medical-records-mandate/#.V5RKxWWibFI.

Forbrukerrådet. “Health and Fitness Apps Violate Users Privacy.” February 25, 2016. Accessed June 20, 2017. http://www.forbrukerradet.no/side/health-and-fitness-apps-violate-users-privacy/.

Frist, William H. “Connected Health and The Rise of The Patient-Consumer.” *Health Affairs* 33, no. 2 (February 2014): 191–93. Accessed June 13, 2017. http://content.healthaffairs.org/content/33/2/191.full.

Gaffney, Alexander. “FDA Targets Companies for Facebook ‘Likes.’ Is Twitter Next?” *RAPS*, August 12, 2014. Accessed June 15, 2017. http://www.raps.org/Regulatory-Focus/News/2014/08/12/20014/FDA-Targets-Companies-for-Facebook-Likes-Is-Twitter-Next/.

Gandhi, Malay, and Teresa Wang. “Digital Health Consumer Adoption: 2015.” *Rock Health*. Accessed June 18, 2017. https://rockhealth.com/reports/digital-health-consumer-adoption-2015/#adoption.

Gartner. “Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016.” February 2, 2016. Accessed June 13, 2017. http://www.gartner.com/newsroom/id/3198018.

Gellman, Robert, and Pam Dixon. “Many Failures: A Brief History of Privacy Self-Regulation in the United States.” *World Privacy Forum*, October 14, 2011. Accessed June 19, 2017. http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf.

Georgetown Law Center on Privacy and Technology. “The Color of Surveillance.” April 8, 2016. Accessed June 20, 2017. https://www.law.georgetown.edu/academics/centers-institutes/privacy-technology/events/.

Goldberg, Rafi. “Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities.” *National Telecommunications and Information Administration*, May 13, 2016. Accessed June 19, 2017. https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

Google. “Healthcare.” *Think with Google*. Accessed June 13, 2017. https://www.thinkwithgoogle.com/intl/en-gb/topics/healthcare.html.

———. “Understanding Advanced Location Options.” *AdWords Help*. Accessed June 18, 2017. https://support.google.com/adwords/answer/1722038?hl=en.

Greer-Smith, Regina. “Smartphone and Mobile Apps: An Important Solution to Increasing Participation and Engagement of Minority and Underserved Communities.” *Blog: National Partnership for Action*, August 22, 2013. Accessed June 13, 2017. https://minorityhealth.hhs.gov/npa/blog/BlogPost.aspx?BlogID=2886.

Gupta, Mayur. “Health Care Marketing Moves from Multichannel to Omnichannel.” *Ad Exchanger*, November 12, 2015. Accessed June 15, 2017. http://adexchanger.com/ad-exchange-news/health-care-marketing-moves-from-multichannel-to-omnichannel/.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

GV. "Portfolio: Life Science and Health." Accessed June 14, 2017. http://www.gv.com/portfolio/#life.

Hoofnagle, Chris. "Privacy Self-Regulation: A Decade of Disappointment." *Electronic Privacy Information Center*, March 4, 2005. Accessed June 19, 2017. http://epic.org/reports/decadedisappoint.html.

"How Can Pharma Firms Market Their Way Back to Growth?" *Knowledge @ Wharton*, April 27, 2016. Accessed June 16, 2017. http://knowledge.wharton.upenn.edu/article/how-can-pharma-firms-market-their-way-back-to-growth/.

"How the HITECH Act Changes HIPAA Compliance." *SearchHealthIT*. Accessed June 19, 2017. http://searchhealthit.techtarget.com/tip/How-the-HITECH-Act-changes-HIPAA-compliance.

IMS Health. "IMS One." Accessed June 15, 2017. http://www.imshealth.com/en/solution-areas/technology-and-applications/ims-one/ims-one-intelligent-cloud.

———. "Nexxus Commercial Application Suite." Accessed June 15, 2017. http://www.imshealth.com/en/solution-areas/healthcare-data-technology-applications/nexxus.

———. "Nexxus Marketing." Accessed June 15, 2017. http://www.imshealth.com/en/solution-areas/technology-and-applications/nexxus/nexxus-marketing.

———. "Orchestrated Customer Engagement: Orchestrate Every Customer Experience to Drive Results." September 2015. Accessed June 15, 2017. http://www.imshealth.com/en/thought-leadership/orchestrated-customer-engagement.

"Innovation in a Patient-Centric World." *PharmaVOICE*, July-August 2015. Accessed June 15, 2017. http://www.pharmavoice.com/article/2015-pharmavoice100-innovation/.

Interlandi, Jeneen. "The Paradox of Precision Medicine." *Scientific American*, April 1, 2016. Accessed June 14, 2017. http://www.scientificamerican.com/article/the-paradox-of-precision-medicine/.

Intouch Solutions. "Patient Engagement in the Instagram Generation: Going Where the Customer Is." April 2016. Accessed June 16, 2017. https://dh1rvgpokacch.cloudfront.net/atavist/57222/document/raw/pharma3dint-1461021121-34.pdf.

Jankowska, M. M., J. Scjhippeerijm, and J. Kerr. "A Framework for Using GPS Data in Physical Activity and Sedentary Behavior Studies." *Exercise and Sport Sciences Review* 43, no. 1 (January 2015): 48–56. Accessed June 13, 2017. http://www.ncbi.nlm.nih.gov/pubmed/25390297.

Jerome, Joseph W. "Buying and Selling Privacy: Big Data's Different Burdens and Benefits." *Stanford Law Review Online* 66 (September 3, 2013): 47–53. Accessed June 21, 2017. http://www.datascienceassn.org/sites/default/files/Buying%20and%20Selling%20Privacy.pdf.

Kaiser, Jocelyn. "NIH's 1-million-volunteer Precision Medicine Study Announces First Pilot Projects." *Science*, February 25, 2016. Accessed June 14, 2017. http://www.sciencemag.org/news/2016/02/nih-s-1-million-volunteer-precision-medicine-study-announces-first-pilot-projects.

Karolefski, John. "Engage Shoppers with Digital Devices." *Progressive Grocer*, January 2016. Accessed June 18, 2017. http://magazine.progressivegrocer.com/i/622765-jan-2016/97.

Kayyali, Basel, David Knott, and Steve Van Kuiken. "The Big-data Revolution in US Health Care: Accelerating Value and Innovation." *McKinsey & Company*, April 2013. Accessed June 20, 2017. http://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-big-data-revolution-in-us-health-care.

Kerr, J., S. J. Marshall, S. Godbole, J. Chen, A. Legge, P. Kelly, M. Oliver, H. M. Badland, and C. Forster. "Using the SenseCam to Improve Classifications of Sedentary Behavior in Free-living Settings." *American Journal of Preventive Medicine* 44, no. 3 (March 2013): 290–296. Accessed June 13, 2017. http://www.ncbi.nlm.nih.gov/pubmed/23415127.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

Krebs, Paul, and Dustin T. Duncan. "Health App Use Among US Mobile Phone Owners: A National Survey." *JMIR mHealth uHealth* 3, n. 4 (October-December 2015): e101. Accessed June 14, 2017. http://mhealth.jmir.org/2015/4/e101/#Introduction.

Krux. "Lookalikes." Accessed June 16, 2017. http://www.krux.com/data-management-platform-solutions/lookalikes/.

The Leadership Conference. "Civil Rights Principles for the Era of Big Data." Accessed June 20, 2017. https://www.law.berkeley.edu/files/Civil_Rights_Principles_for_the_Era_of_Big_Data_FINAL(1).pdf.

Lecher, Colin. "The FDA Doesn't Want to Regulate Wearables, and Device Makers Want to Keep It That Way." *The Verge*, June 24, 2015. Accessed June 19, 2017. http://www.theverge.com/2015/6/24/8836049/fda-regulation-health-trackers-wearables-fitbit.

Ledger, Dan. "Inside Wearables—Part 3." *Endeavour Partners*, January 2016. Accessed June 13, 2017. https://www.yumpu.com/en/document/view/56058196/inside-wearables-part-3.

Lee, Kristen. "Wearable Health Technology and HIPAA: What Is and Isn't Covered." *SearchHealthIT*. Accessed June 19, 2017. http://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered.

Leonhard, Gerd. "Big Data, Big Business, Big Brother?" *CNN*, February 26, 2013. Accessed June 14, 2017. http://edition.cnn.com/2014/02/26/business/big-data-big-business/.

Lewis, R.J. "Advertising Targeting for Healthcare & Life Sciences in the 21st Century." *CBI Blog*, May 11, 2015. Accessed June 18, 2017. http://blog.cbinet.com/blog/advertising-targeting-for-healthcare-life-sciences-in-the-21st-century.

LiveRamp. "Look-alike Modeling: The What, Why, and How." Accessed June 16, 2017. http://liveramp.com/blog/look-alike-modeling-the-what-why-and-how/.

Lohr, Steve. "Trump Completes Repeal of Online Privacy Protections From Obama Era." *New York Times*, April 3, 2017. Accessed June 19, 2017. https://www.nytimes.com/2017/04/03/technology/trump-repeal-online-privacy-protections.html?_r=0.

Lotame. "1st Party Data, 2nd Party Data, 3rd Party Data: What Does It All Mean?" November 10, 2013. Accessed June 19, 2017. https://www.lotame.com/resource/1st-party-2nd-party-3rd-party-data-what-does-it-all-mean/.

Maddox, Teena. "Top IoT and Wearable Tech Trends for 2016: Smartwatches in Transition as Smartglasses Rule." *TechRepublic*, January 14, 2016. Accessed June 13, 2017. http://www.techrepublic.com/article/top-iot-and-wearable-tech-trends-for-2016-smartwatches-in-transition-as-smartglasses-rule/.

Mantelero, Alessandro. "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): 238–55. Accessed June 20, 2017. http://staff.polito.it/alessandro.mantelero/Mantelero_Personal_data_for_decsional_purposes_CLSR_2016.pdf.

Martin, Chuck. "Tapping Wearables Data: 38% of Marketers Want Daily Routine, 37% Precise Location." *Media Post IoT Daily Connected Thinking*, April 28, 2016. Accessed June 15, 2017. http://www.mediapost.com/publications/article/274547/tapping-wearables-data-38-of-marketers-want-dail.html.

Mayer-Schönberger, Viktor, and Kenneth Cukier. *Big Data: A Revolution that Will Transform how we Live, Work, and Think*. New York: Houghton Mifflin Harcourt, 2013.

McCaffrey, Kevin. "Remedy Health Media Launches New Series: A Peek into Patients' Lives." *Medical Marketing & Media*, 15 June 2016. Accessed June 18, 2017. http://www.mmm-online.com/media-news/remedy-health-media-launches-new-series-a-peek-into-patients-lives/article/503104/.

Meingast, Marci, Tanya Roosta, and Shankar Sastry. "Security and Privacy Issues with Health Care Information Technology." *Conference Proceedings of the IEEE Engineering in*

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

Medicine and Biology Society 1 (2006): 5453–58. Accessed June 19, 2017. http://www.cs.jhu.edu/~sdoshi/jhuisi650/discussion/secprivhealthit.pdf.

"Minority Report—Personal Advertising in the Future." *YouTube*, December 7, 2010. Accessed June 19, 2017. https://www.youtube.com/watch?v=7bXJ_obaiYQ.

Mitchell, Rick. "IP Addresses Are Protected Personal Data, EU Top Court Rules." *Bloomberg Law: Privacy & Data Security*, October 19, 2016. Accessed June 20, 2017. http://www.bna.com/ip-addresses-protected-n57982079024/.

Mitchell, Shane, Nicola Villa, Martin Stewart-Weeks, and Anne Lange. "The Internet of Everything for Cities." *Cisco*, 2013. Accessed June 13, 2017. http://www.cisco.com/web/about/ac79/docs/ps/motm/IoE-Smart-City_PoV.pdf.

Mittelstadt, Brent Daniel, and Luciano Floridi. "The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts." *Science and Engineering Ethics* 22, n. 2 (May 23, 2015): 303–41.

Moked, Karen. "Digilant Launches Consumer Persona Data Solution for Pinpointing New Audiences Programmatically." June 16, 2015. Accessed June 13, 2017. http://www.digilant.com/digilant-launches-consumer-persona-data-solution-for-pinpointing-new-audiences-programmatically/.

Montgomery, Kathryn C. "Safeguards for Youth in the Digital Marketing Ecosystem." In *Handbook of Children and the Media*, second edition. Edited by Dorothy G. Singer and Jerome L. Singer, 631–48. Thousand Oaks, CA: Sage Publications, 2011.

Montgomery, Kathryn C., Jeff Chester, and Katharina Kopp. "Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection." 2016, 42–47. Accessed June 22, 2017. https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf.

Munro, Dan. "Data Breaches in Healthcare Totaled Over 112 Million Records In 2015." *Forbes*, December 13, 2015. Accessed June 14, 2017. http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#72f81067fd5a.

Murdough, C. "Social Media Measurement: It's Not Impossible." *Journal of Interactive Advertising* 10, n. 1 (2009): 94–99.

National Cancer Institute. "Cancer Moonshot." Accessed June 13, 2017. http://www.cancer.gov/research/key-initiatives/biden-cancer-initiative.

National Science and Technology Council. "National Privacy Research Strategy." June 2016. Accessed June 19, 2017. https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf.

Nielsen. "It's Thanksgiving, Please Pass the Smartphone." November 24, 2015. Accessed June 13, 2017. http://www.nielsen.com/us/en/insights/news/2015/its-thanksgiving-please-pass-the-smartphone.html.

O'Dea, Jim. "The Pharmacy's New Role in Providing Healthcare Services." *PM360*, January 23, 2014. Accessed June 18, 2017. https://www.pm360online.com/the-pharmacys-new-role-in-providing-healthcare-services/.

Office of the National Coordinator for Health Information Technology, Department of Health and Human Services. "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap." *Version 1.0*. Accessed June 14, 2017. https://www.healthit.gov/policy-researchers-implementers/interoperability.

———. "Understanding the Impact of Health IT in Underserved Communities and those with Health Disparities." May 2013. Accessed June 13, 2017. https://www.healthit.gov/sites/default/files/hit_disparities_report_050713.pdf.

Oracle. "Navigating the New Prescriber's Path." Accessed June 19, 2017. https://www.oracle.com/marketingcloud/gatedform/gated-content-overlay-content.html?elqoffer=NavigatingNewPrescribersPath-LifeSci_2015.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

———. "Oracle Data Cloud: Data Directory," 2016. Accessed June 19, 2017. http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf.

———. "Oracle Marketing Cloud for Life Sciences: Personalize Life Sciences Communications for Healthcare, Pharma, Biotech, and Medical Devices." Accessed June 19, 2017. https://www.oracle.com/marketingcloud/products/life-sciences.html.

Organization for Economic Cooperation and Development. "*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*." Accessed June 21, 2017. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Orsini, Patricia. "The US Healthcare and Pharma Industry 2016." *eMarketer*, May 12, 2016. Author's personal copy.

"Partner Forum: Are Wearables a Pharma Field Day?" *Medical Marketing & Media*, 1 August 2015. Accessed June 15, 2017. http://www.mmm-online.com/features/partner-forum-are-wearables-a-pharma-field-day/article/428202/.

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

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

Patient Privacy Rights Foundation. "Privacy Trust Framework." Accessed June 19, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2231667.

Peel, Deborah. "An Implementation Path to Meet Patients' Expectations and Rights to Privacy and Consent." In *Information Privacy in the Evolving Healthcare Environment*. Edited by Linda Koontz, 89–116. Chicago: Healthcare Information and Management Systems Society, 2013.

Pentland, Alex, 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. Accessed June 18, 2017. https://kit.mit.edu/sites/default/files/documents/WISH_BigData_Report.pdf.

PricewaterhouseCoopers. "The Wearable Future." November 2014. Accessed June 14, 2017. https://www.pwc.com/mx/es/industrias/archivo/2014-11-pwc-the-wearable-future.pdf.

Privacy Rights Clearinghouse. "Fact Sheet 8a: Health Privacy: HIPAA Basics." Accessed June 19, 2017. https://www.privacyrights.org/content/health-privacy-hipaa-basics.

"Privacy Rights Clearinghouse Releases Study: Mobile Health and Fitness Apps: What Are the Privacy Risks?" July 15, 2015. Accessed June 20, 2017. https://www.privacyrights.org/mobile-medical-apps-privacy-alert.

PwC. "New Health Economy Vision for the Future." Accessed June 14, 2017. http://www.pwc.com/us/en/health-industries/health-research-institute/publications/new-health-economy-vision-for-the-future.html.

Quantified Self. "About the Quantified Self." Accessed June 13, 2017. http://quantifiedself.com/about/.

Ransbotham, Sam. "Coca-Cola's Unique Challenge: Turning 250 Datasets into One." *MIT Sloan Management Review*, May 27, 2015. Accessed June 63, 2017. http://sloanreview.mit.edu/article/coca-colas-unique-challenge-turning-250-datasets-into-one/.

Remedy Health Media. "Our Brands." Accessed June 18, 2017. http://www.remedyhealthmedia.com/brands-partners.

Robert Wood Johnson Foundation. "From Vision to Action: A Framework and Measures to Build a Culture of Health." *Fall*, 2015. Accessed June 20, 2017. http://www.rwjf.org/content/dam/COH/RWJ000_COH-Update_CoH_Report_1b.pdf.

———. "What is a Culture of Health?" *Evidence for Action*. Accessed June 20, 2017. http://www.evidenceforaction.org/what-culture-health.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

Ryan, Tom. “Has Mobile Created a New Marketing Moment of Truth?” *CPGmatters*, October 2015. Accessed June 18, 2017. http://www.cpgmatters.com/RetailTrends101915.html.

Samsung. “Policy Gets Personal.” *Washington Post*, 2015. Accessed June 13, 2017. http://www.washingtonpost.com/sf/brand-connect/samsung.

Shelfbucks. “The Future of Retailing...Brought to You by Shelfbucks.” Accessed June 18, 2017. http://www.shelfbucks.com/complete-your-omni-channel-strategy.

Sicular, Svetlana. “Gartner’s Big Data Definition Consists of Three Parts, Not to be Confused with Three ‘V’s.” *Forbes*, March 27, 2013. Accessed June 14, 2017. http://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/.

Skyhook. “SDK Data Previews.” Accessed June 16, 2017. https://resources.skyhookwireless.com/wiki/type/documentation/context-accelerator/sdk-data-previews/3997879.

Sloan, Robert H., and Richard Warner. “Beyond Notice and Choice: Privacy, Norms, and Consent.” *The Journal of High Technology Law* 14, no. 2 (July 2014): 370–414. Accessed June 20, 2017. https://www.suffolk.edu/documents/jhtl_publications/SloanWarner.pdf.

Smith, Cooper. “Reinventing Social Media: Deep Learning, Predictive Marketing, And Image Recognition Will Change Everything.” *Business Insider*, March 20, 2014. Accessed June 14, 2017. http://www.businessinsider.com/social-medias-big-data-future-2014-3.

Snider, Mike. “Online Ad Spending to Top TV Ads in 2017.” *USA Today*, June 8, 2016. Accessed June 16, 2017. http://www.usatoday.com/story/tech/news/2016/06/08/online-ad-spending-top-tv-ads-2017/85594160/.

Solove, Daniel J. “Privacy Self-Management and the Consent Dilemma.” *Harvard Law Review* 126 (2013): 1880-1903. Accessed June 21, 2017. http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2093&context=faculty_publications.

Son, Sooel, Daehyeok Kim, and Vitaly Shmatikov. “What Mobile Ads Know About Mobile Users.” *NDSS*, 2016. Accessed June 18, 2017. http://www.cs.cornell.edu/~shmat/shmat_ndss16.pdf.

Spinelli, Cooper J. “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). Accessed June 19, 2017. http://digitalcommons.wcl.american.edu/lpb/vol6/iss1/3.

Stables, James. “Fitness Trackers Are in a Race to the Bottom.” *Wareable*, June 16, 2016. Accessed June 13, 2017. http://www.wareable.com/fitness-trackers/fitness-trackers-are-in-a-race-to-the-bottom.

Staton, Tracy. “Pharma’s Ad Spend Vaults to $4.5B, with Big Spender Pfizer Leading the Way.” *Fierce Pharma*, March 25, 2015. Accessed June 16, 2017. http://www.fiercepharma.com/dtc-advertising/pharma-s-ad-spend-vaults-to-4-5b-big-spender-pfizer-leading-way.

“Strategic Pharma Solutions, Inc. Continues to Grow Digital Offerings through Expansion of Talent Base.” September 11, 2015. Accessed June 15, 2017. 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.

Sutton, Sam. “Google Ventures Eyes Intersection of Healthcare, Data with Zephyr Investment–VCJ Deal News.” *The PE Hub Network*, August 21, 2015. Accessed June 14, 2017. https://www.pehub.com/2015/08/google-ventures-eyes-intersection-of-healthcare-data-with-zephyr-investment-vcj-deal-news/.

Sweeney, Latanya. “Only You, Your Doctor, and Many Others May Know.” *Technology Science*, September 29, 2015. Accessed June 19, 2017. http://techscience.org/a/2015092903/.

TapSense. “TapSense Launches Industry’s First Programmatic Ad Platform for Apple Watch.” January 4, 2015. Accessed June 15, 2017. http://www.tapsense.com/blog/post/tapsense-launches-industrys-first-programmatic-ad-platform-apple-watch.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

Target. "Target Kicks off New Team Member Wellness Initiatives." *A Bullseye View*, September 16, 2015. Accessed June 13, 2017. https://corporate.target.com/article/2015/09/team-member-wellness.

Terry, Nicolas. "Big Data Proxies and Health Privacy Exceptionalism." *Health Matrix—Journal of Law-Medicine* 24 (2014): 65–108. Accessed June 19, 2017. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320088#%23.

———. "Health Privacy is Difficult but Not Impossible in a Post-HIPAA Data-Driven World." *CHEST Journal* 146, no. 3 (2014): 835, doi:10.1378/chest.13-2909.

———. "Protecting Patient Privacy in the Age of Big Data." *University of Missouri-Kansas City Law Review* 81, no. 2 (2012). Accessed June 19, 2017. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2153269.

Topol, Eric. *The Patient Will See You Now: The Future of Medicine is in Your Hands*. New York: Basic Books, 2015.

TPG Rewards. "TPG's Tap to Win Technology." Accessed June 18, 2017. http://taptopromo.com/.

"Transformational Technology." *Pharmaceutical Market Europe*, May 2016. Accessed June 15, 2017. http://www.pmlive.com/digital_edition/pme/pharmaceutical_market_europe_-_may_2016.

Tufekci, Zeynep. "Engineering the Public: Big Data, Surveillance and Computational Politics." *First Monday* 19, n. 7 (July 2014). Accessed June 14, 2017. http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097.

Turow, Joseph. "Americans and Online Privacy: The System is Broken." Annenberg Public Policy Center of the University of Pennsylvania, June 2003. Accessed June 20, 2017. http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.

———. *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth*. New Haven: Yale University Press, 2013.

Turow, Joseph, 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. Accessed June 19, 2017. https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and.

UC Berkeley Center for Long-Term Cybersecurity. "Scenario Four: Intentional Internet of Things." Accessed June 18, 2017. https://cltc.berkeley.edu/scenario/scenario-four/.

Under Armour, "MapMyFitness Virtual Fitness Challenge." Accessed June 15, 2017. http://advertising.underarmour.com/products/challenges/mapmyfitness-challenge.

———. "Mobile Interstitials." Accessed June 15, 2017. http://advertising.underarmour.com/products/media/mobile-interstitial.

———. "Our Platform." Accessed June 15, 2017. http://advertising.underarmour.com/#platform.

———. "Our Products." Accessed June 15, 2017. http://advertising.underarmour.com/products/.

Upturn. "Civil Rights, Big Data, and Our Algorithmic Future." September 2014. Accessed June 19, 2017. https://bigdata.fairness.io/wp-content/uploads/2015/04/2015-04-20-Civil-Rights-Big-Data-and-Our-Algorithmic-Future-v1.2.pdf.

"The U.S. Consumer Wearables Market Will Reach $9.7B by 2019, Says Compass Intelligence." *Market Wired*, October 20, 2015. Accessed June 13, 2017. http://www.marketwired.com/press-release/the-us-consumer-wearables-market-will-reach-97b-by-2019-says-compass-intelligence-2065369.htm.

U.S. Department of Health and Human Services. "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA." Accessed June 20, 2017. https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

Federal Trade Commission, "Big Data: A Tool for Inclusion or Exclusion?" January 2016. Accessed June 20, 2017. https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

———. "Internet of Things—Privacy & Security in a Connected World." January 2015. Accessed June 20, 2017. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

———. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers." March 2012. Accessed June 20, 2017. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

U.S. Food and Drug Administration. "Keeping Watch Over Direct-to-Consumer Ads." Accessed June 15, 2017. http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm107170.htm.

———. "Webinar— Final Guidance on 'General Wellness: Policy for Low-Risk Devices.'" September 1, 2016. Accessed June 19, 2017. http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm515955.htm.

"US$ 24 Billion Worth of Wearable Medical Devices Expected to be Sold in 2016: Future Market Insights (FMI)." *PR Newswire*, June 6, 2016. Accessed June 13, 2017. 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.

Venrock. "Portfolio." Accessed June 14, 2017. http://www.venrock.com/portfolio/.

Ventola, C. Lee. "Direct-to-Consumer Pharmaceutical Advertising: Therapeutic or Toxic?" *Pharmacy & Therapeutics* 36, no. 10 (October 2011): 681–84. Accessed June 16, 2017. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3278148/.

Walgreens. "Health Apps & Devices." Accessed June 18, 2017. https://www.walgreens.com/steps/appmarket.jsp.

Wasserman, Emily. "Verily Tapped by NIH to Launch Obama's Precision Medicine Initiative." *Fierce Biotech*, February 25, 2016. Accessed June 14, 2017. http://www.fiercemedicaldevices.com/story/verily-tapped-nih-launch-obamas-precision-medicine-initiative/2016-02-25.

Wharton School, University of Pennsylvania; McKinsey and Company; and Google. *Pharma 3D: Rewriting the Script of Marketing in the Digital Age*. 2016. Accessed June 16, 2017. http://www.pharma3d.com/#chapter-856435.

The White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," *Journal of Privacy and Confidentiality* 4, n. 2 (2012): 95–142. Accessed June 20, 2017. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=jpc.

———, "FACT SHEET: Cybersecurity National Action Plan," February 9, 2016. Accessed June 20, 2017. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

———, "Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights," February 23, 2012. Accessed June 20, 2017. https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b.

———, "PCAST Releases Report on Big Data and Privacy," May 1, 2014. Accessed June 20, 2017. https://www.whitehouse.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy.

———. "Precision Medicine Initiative: Guiding Principles for Protecting Privacy and Building Trust." November 9, 2015. Accessed June 14, 2017. https://www.whitehouse.gov/precision-medicine#section-principles.

———, "We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online," February 23, 2012. Accessed June 20, 2017.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms

http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

White House Office of the Press Secretary. "FACT SHEET: Obama Administration Announces Key Actions to Accelerate Precision Medicine Initiative." February 25, 2016. Accessed June 14, 2017. https://www.whitehouse.gov/the-press-office/2016/02/25/fact-sheet-obama-administration-announces-key-actions-accelerate.

WireSpring Technologies. "POP Displays." Accessed June 18, 2017. https://www.wirespring.com/Solutions/pop_displays.html.

World Privacy Forum. "Health Privacy." Accessed June 19, 2017. https://www.worldprivacyforum.org/category/health-privacy/.

———. "New WPF Report—The Precision Medicine Initiative and Privacy: Will Any Legal Protections Apply?" May 18, 2016. Accessed June 20, 2017. https://www.worldprivacyforum.org/2016/05/wpf-report-the-precision-medicine-initiative-what-laws-apply/.

———. "Precision Medicine Initiative." May 17, 2016. Accessed June 13, 2017. https://www.worldprivacyforum.org/category/precision-medicine-initiative/.

Xaxis. "A GeoMarketing Conversation with MoPub, Xaxis, VivaKi, and Factual." December 10, 2014. Accessed June 18, 2017. 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. Accessed June 18, 2017. https://www.xaxis.com/press/view/xaxis-launches-light-reaction-mobile-first-performance-business-with-innova.

"Your Health Records: About Blue Button." HealthIT.gov. Accessed June 14, 2017. https://www.healthit.gov/patients-families/blue-button/about-blue-button.

Zamora, Alyssa. "Obese Workers Cost More Than Healthcare, Absenteeism." *Duke Today*, October 8, 2010. Accessed June 13, 2017. https://today.duke.edu/2010/10/workobese.html.

This content downloaded from 136.165.155.231 on Tue, 02 Oct 2018 18:44:06 UTC
All use subject to https://about.jstor.org/terms