Contextual Expectations of Privacy in Self-Generated Health Information Flows

Heather Patterson

New York University
Media, Culture, and Communication
Information Law Institute

I. Introduction

Converging technological, regulatory, and social forces point to an increasingly personalized, data driven, and collaborative future of health decision-making.[1] A prominent driver[2] of this transition is the ready availability of low-cost, off-the-shelf commercial digital self-monitoring sensors and apps that enable individuals to log broad swaths of highly granular behavioral and physiological health attributes in near real time. Mobile health self-quantification tools, including smart pedometers,[3] calorie counters,[4] heart rate monitors,[5] sleep trackers,[6] and other "participatory personal data"[7] collection devices hold great promise for individuals and for the public health, including increased bodily awareness, proactive health engagement, and community building. Their commercial implementation also raises significant privacy and security issues that warrant close attention.

Self-quantification services collect, process, and share an unprecedented amount of

[1] For one vision of the future of health care, see Eric Topol, *The Creative Destruction of Medicine: How the Digital*

[2] *See e.g.*, Jeffery Norris, *Self-Tracking May Become Key Element of Personalized Medicine*, UCSF NEWS, Oct. 5, 2012, at http://www.ucsf.edu/news/2012/10/12913/self-tracking-may-become-key-element-personalized-medicine) ("At [Medicine X 2012, a three-day conference on social media and information technology's potential impact on medicine] at Stanford University…attendees and presenters — including two UCSF physicians — asserted not only that self-tracking can help patients to improve their lives, but also that self-tracking has the potential to change medical practice and the relationship between patients and their health care providers.").

[3] E.g., Fitbit (http://www.fitbit.com/); Phillips DirectLife (http://www.directlife.philips.com/).

[4] E.g., Bodybugg (www.bodybugg.com/); BodyMedia (http://www.bodymedia.com/?whence=).

[5] E.g., CardioNet (https://www.cardionet.com/); LifeWatch (http://www.lifewatch.com/).

[6] E.g., Zeo (http://www.myzeo.com/sleep/).

[7] Terminology for ubiquitous personal data collection is varied; for an up-to-date summary, see Katie Shilton, *Participatory Personal Data: An Emerging Research Challenge for the Information Sciences*, JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE AND TECHNOLOGY, preprint dated 2012. ("Because using ubiquitous digital tools for data capture is a relatively new activity, the terminology used to describe this research is varied, going under names including mobile health or mHealth, self-quantifying, self- surveillance, participatory sensing, and urban sensing….What unifies these projects is the data they collect: *participatory personal data*.") (citations omitted).

highly intimate details about consumers' bodies and behaviors that historically have been confined to the relatively secure and protected spheres of the home and the professional health care organization. Beyond concerns about the sheer quantity and detail of self-generated data lie worries about its containment and use: Information may now flow far beyond the traditional patient-to-physician path—for example, it may flow via individual users to community groups, social networks, and cloud-based personal health portfolios; it may flow via companies themselves to business associates, partner insurers and employers, and data brokers. The scale, scope, and nontraditional flows of health information, coupled with sophisticated data mining techniques that support reliable health inferences, put consumers at risk of embarrassment and reputational harm, employment and insurance discrimination, and unwanted behavioral marketing.

Privacy risks are compounded by current regulatory gaps. Conceptually, consumer oriented wellness and health tools occupy the intersection between the traditional clinical medical and commercial marketplaces. Where mobile health is concerned, offices within the Department of Health and Human Services (HHS) that have historically assumed responsibility for assuring consumer privacy and safety in health technologies (including the Office for Civil Rights (OCR), which enforces HIPAA, the Office of National Coordinator for Health Information Technology (ONC), which coordinates nationwide efforts to implement health information technology, and the Food and Drug Administration (FDA), which oversees the safety of medical devices), appear to be continuing to focus narrowly on medical tools. Where they engage with self-quantification services, for example, current efforts focus on mobile *medical* apps or mobile devices used in the health care sector, by health care providers, for the provision of care.[8] This leaves privacy issues involving commercial health quantification tools used by laypersons to be addressed by federal and state agencies regulating consumer privacy more broadly.

[8] See e.g., Mobile Devices Roundtable: Safeguarding Health Information, Real World Usages and Real World Privacy and Security Practices, THE OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, March 16, 2012, page 15, lines 17-21 at http://www.healthit.gov/sites/default/files/mobile_device_transcript_ocpo_rev_4.pdf ("And we will be focusing today, as Dr. Mostashari mentioned, on the privacy and security of mobile devices as they are used in the health care sector by health care providers for providing care.").

.

Fortunately, there is now a strong unified push by federal and state entities to develop broad and comprehensive protections for consumer privacy. Although these efforts are occurring outside of the health care context, they will encompass mobile self-quantification health and wellness tools simply by virtue of being geared toward commercial online and mobile technology. The White House's February 2012 Consumer Privacy Bill of Rights, for example, sets forth a set of privacy principles based on the Fair Information Practice Principles (FIPPs) that is intended to provide a clear baseline of privacy protections for consumers *online*, and particularly in commercial sectors not currently subject to existing Federal information privacy laws. A recent FTC staff report, issued in in February 2013, recommends that mobile platforms, app developers, advertising networks and other third parties improve privacy disclosures to users of mobile technologies, including smart phones and apps.[9] The State of California, traditionally a leader in privacy, has also vigorously embraced consumer privacy protections in information collected and distributed online, going so far as to take the position that mobile apps are "commercial Web site(s) or online service(s)" covered by the California Online Privacy Protection Act of 2003 (CalOPPA).[10]

These new guidelines and recommendations have the potential to improve privacy and security for users participating in commercial activity on the Internet across multiple business sectors. Particularly important is the Administration's Consumer Privacy Bill of Rights, which recognizes that consumers often engage with technology differently as a function of the social contours of a particular business sector or environments. Customary information flow norms and use practices—including the type, frequency, breadth, and depth of interactions—that predominate in one online environment, such as a social networks, may vary widely from those that predominate in online retail, gaming, or therapeutic support communities. These differential engagements may have a profound impact on expectations regarding information collection and flow.

[9] *Mobile Privacy Disclosures: Building Trust Through Transparency*
[10] Kamala D. Harris, Template Notice of Non-Compliance with California Online Privacy Protection Act, Oct. 26, 2012, at http://oag.ca.gov/system/files/attachments/press_releases/CalOPPA%20Letter_0.pdf.

Contextual expectations of data collection and flow are explicitly recognized in the Privacy Bill of Rights' third Principle, *Respect for Context*, which urges that, "Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent *with the context in which consumers provide the data*." The conceptual underpinning of this Principle is the framework of Contextual Integrity,[11] which posits that individuals are exquisitely sensitive to context-dependent social norms that govern the appropriateness of information flows. Contextual integrity predicts that individuals hold granular and finely-tuned information-sharing preferences that vary by the *type* of information to be shared, by the *recipient* of that information, and by the *transmission principles* that inhere in the social context in which individuals provide their data, such as expectations of confidentiality (as with a doctor-patient relationship) or reciprocity (as with a friendship).

The White House notes that Respect for Context "requires companies to consider carefully:

- what consumers are likely to understand about their data practices based on the products and services they offer,
- how the companies themselves explain the roles of personal data in delivering them,
- research on consumers' attitudes and understandings, and
- feedback from consumers.

Context should also "help to determine which personal data uses are likely to raise the greatest consumer privacy concerns."[12]

This paper is the first of a series of reports relaying empirical observations of consumers' attitudes and understandings about data use practices in the commercial mobile health

[11] *See* Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. STANFORD UNIVERSITY PRESS, 2010.

[12] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE HOUSE, Feb. 23, 2012, at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

environment. Here, I outline privacy risks that inhere in the commercial mobile health environment and summarize findings from structured qualitative interviews regarding individuals' real-world use of health and wellness self-quantification tools. I have focused on information collected from twenty-one users of a popular health self-tracking tool, the Fitbit. The purpose of this initial paper is to give policy makers, privacy scholars, and commercial entities a glimpse into the health self-tracking social context, including how consumers engage with health self-tracking devices, what information flow expectations they bring to their interactions, which specific health information flows individuals flag as concerning or potentially threatening, and how attempts to protect the privacy and security of their own health information have succeeded and failed.

The paper proceeds as follows: In Section II, I very briefly summarize the wide range of health self-tracking sensors and apps available to consumers and describe well-known benefits and risks associated with the use of these tools. In Section III, I explain current regulatory gaps regarding the consumer-facing mobile health ecosystem. In Section IV, I relay privacy and security vulnerabilities that emerged from these conversations, including specific concerns that self-tracking individuals raised regarding their commercial mobile health expectations and use. At the end of each observation, I offer straightforward, targeted, and easily implemented solutions to assist entities seeking practical guidance in this relative unregulated space.

These guidelines are provided not only for the sake of the individual user. Keeping health information secure builds consumer trust and encourages broader adoption of new health and wellness technologies, furthering the development and dissemination of critical new information regarding the public's health and well-being.

II. Commercial Health and Wellness Tools Present Benefits and Risks to Consumers

Tools that enable health self-tracking are widely available and affordable even to non-tech-savvy, fitness-minded individuals. Currently, over 200 health sensors[13] and 97 thousand mobile health apps[14] are available for download or purchase. Some are geared towards health care providers who are increasingly using them as part of their own clinical practice,[15] but about 70% are consumer-focused.[16] Many specialize in helping consumers track their weight, diet, or exercise,[17] but others encompass a broad range of information types, including detailed longitudinal portraits of individuals' states,[18] behaviors,[19] signals of clinical conditions,[20] physiological biomarkers,[21] personal goals,[22] and even real-time geospatial locations while walking, running, or cycling.[23] And although first generation tools are largely app or single-sensor based (e.g., accelerometer, potentiometer, GSR, or GPS), one trend is toward the development of multi-sensor platforms, e.g., the integration of mood tracking and social interaction data, or personal genetic risk and blood serum levels, or weight, exercise, and food consumption data. Further, the development of sophisticated wearable body textiles, handheld blood analyzers, monitoring patches in the form of stretchable tattoos, and glucose monitoring systems, among other tools, is currently underway.

Benefits

Health self-tracking holds great promise for individuals and society. In addition to fostering greater self-awareness and health accountability, the practice of tracking one's

[13] Brian Dolan, *Mobile Health Sensor Market to Hit $5.6B by 2017*, MOBIHEALTHNEWS, April 24, 2013, at http://mobihealthnews.com/21878/mobile-health-sensor-market-to-hit-5-6b-by-2017/.

[14] Jonah Comstock, *Report: 1.7B to Download Health Apps by 2017*, MOBIHEALTHNEWS, March 14, 2013, at http://mobihealthnews.com/20814/report-1-7b-to-download-health-apps-by-2017/.

[15] *See e.g.*, Happtique, a company that runs a voluntary health app certification program to make app selection easier for clinical health care providers, at http://www.happtique.com/.

[16] http://www.globaldata.com/PressReleaseDetails.aspx?PRID=294&Type=Industry&Title=Medical+Devices.

[17] Susannah Fox and Maeve Duggan, *Tracking for Health*, THE PEW INTERNET AND AMERICAN LIFE PROJECT, Jan. 28, 2013, at http://www.pewinternet.org/Reports/2013/Tracking-for-Health/Main-Report/Seven-in-ten-US-adults-track-a-health-indicator-for-themselves-or-for-a-loved-one.aspx.

[18] *E.g.*, height, weight, body mass index, reproductive health

[19] *E.g.*, dietary habits, fitness, sleep cycles, sexual activities

[20] *E.g.*, diabetes, asthma, hypothyroidism, chronic pain

[21] *E.g.*, glucose levels, blood pressure, heart rates, cholesterol

[22] E.g., smoking cessation, alcohol reduction, mood improvements

[23] *See e.g.*, Endomondo, at http://www.endomondo.com/login.

health metrics allows users to find meaningful correlations between diet, exercise, sleep, and mental, physical, and cognitive well-being. Tracking also promotes community building and information sharing. Users of the Fitbit, for example, have taken more than 80 billion steps with the device since the company launched five years ago,[24] but many find that its real appeal lies in its infographic-heavy web based dashboard, fitness "badges," competition-and-collaboration leaderboards, and discussion groups that encourage online community building.[25] Finally, there is broad consensus[26] among computer scientists and others that self-tracking may have positive public health benefits. Multiple "small data" streams generated by health and other sensor networks logging clinical and environmental data may one day be integrated to reduce medical inefficiencies such as redundant lab tests, and be used to simplify the management of chronic conditions like diabetes, asthma, and heart disease. Integrated data streams can inform individual care plans, and may also identify population-level health issues, such as epidemics or previously unreported drug interactions, earlier and more efficiently than clinical trials.[27]

Risks

Ubiquitous Monitoring. Although health self-tracking tools provide significant benefits to consumers, they also present new and challenging threats to privacy and security. First, wearable health sensor and apps enable the ubiquitous collection of large amounts of behavioral data in real time. Continuous tracking facilitates the construction of a full complement of detailed user behaviors, including when people wake up, weigh themselves, bathe, eat, leave the home for work, engage in various forms of exercise, recreate, and sleep. Sleep quality and duration, food intake patterns, exercise preferences, and drinking habits—particularly if combined with geospatial location by virtue of an accompanying smart phone app with location features enabled, support reliable

[24] Jennifer Wang, *How Fitbit Is Cashing in on the High-Tech Fitness Trend*, Entrepreneur, July 28, 2012, at http://www.entrepreneur.com/article/223780; http://www.fastcompany.com/most-innovative-companies/2012/fitbit.

[25] *E.g.,* Fitbit Community, at http://www.fitbit.com/community.

[26] *See e.g*., UCSF's Center for Digital Health Innovation at http://centerfordigitalhealthinnovation.org/; UCLA's Center for Embedded Sensing (CENS) at http://research.cens.ucla.edu/; Dartmouth's Smartphone Sensing Group at http://sensorlab.cs.dartmouth.edu/index.html; MIT's Institute for Medical Engineering and Science at http://imes.mit.edu/ and Open mHealth at http://openmhealth.org/.

[27] *See e.g*., Deborah Estrin, Sensemaking for Mobile Health, NYU Campus Lecture, May 2, 2103, announcement at http://wiseli.engr.wisc.edu/celebrating/Estrin_Events.pdf.

inferences about physical and mental health over time…and more. Are you chronically ill? Well? Happy? Anxious? Depressed? Do you regularly suffer from insomnia? Are you particularly busy at work this quarter? Are you feeling better or worse than last week? Are your heart rate and cholesterol suddenly off target for somebody of your age and fitness level? Are you infertile? Could you be having an affair? In short, ubiquitous wearing encourages users treat every moment of their lives as an opportunity to log information about their physical self, and results in startlingly complete profiles of an individuals longitudinal behavioral patterns over periods of weeks, months, or longer.

Granular Information Collection. Second, many wearable sensors and apps are able to capture an enormous variety and detail of information about demographic, physiological, and behavioral attributes of an individual. Even seemingly-innocuous "fitness" services collect a large amount of information: When first establishing a Fitbit account, for example, users supply their first and last name and preferred nickname; their zip code, city, state, and country; their gender and date of birth; their height, weigh, and stride length; and a personal photograph and "about me" text. They then synch their personal Fitbit tracking device to their newly-established account.

The Fitbit One, by far most commonly used tracker among study participants, records daily logs and weekly averages of steps taken, distance traveled, calories burned, floor climbed, hours slept, number of times awoken, and sleep efficiency. Users are supplied with opportunities, on their personalized Fitbit.com dashboard accessed via the Fitbit.com website or the Fitbit Android or iPhone app, to manually track their physical activities (name of activity, when they engaged in it and for how long); foods eaten (brand, amount, calorie count, nutritional value, and whether consumed as breakfast, lunch, dinner, or snacks); weight updates (weight, percent body fat, and BMI); bodily measurements (neck, biceps, forearm, chest, waist, hips, thigh, and calf); blood pressure and blood glucose levels (morning, afternoon, and evening), and heart rate (resting, normal, and active, with associated times of day).

Many of these metrics are plotted against benchmarks: a user-provided primary weight goal and a corresponding Fitbit-generated "food plan." Space within an online journal is provided to record moods and allergies, and to enter freeform text. Users also have the option to log any number of metrics of their choosing, such as alcohol or tobacco use. Encouraging this kind of rigorous, whole-body quantification of the self not only habituates individuals to the concept and practice of scanning and cataloging activity and consumption habits, it results in corporations holding vast treasure troves of highly personal health data about tens of thousands of users—health and wellness libraries with unprecedented and complete entries of incalculable value to business associates, employers, and insurance companies.

Decontextualized Information Flows. Third, wellness and health tracking tools enable novel and potentially harmful health information flows. Historically, individuals have disclosed their most sensitive health data primarily to trusted family, friends and care advisors in the home or in the controlled environment of the clinical operatory. Patients may expect limited types and quantities of their health information to be shared within and outside the physician's office for carefully-cabined administrative, insurance, and pharmaceutical purposes, but they are also able to rely on a number of other cues—clinicians' professional training, codes of ethics, structural aspects of the medical encounter itself, hazy knowledge of legal protections—to trust that in the canonical and idealized case, their health data will be used diagnostically, only as needed, and not shared beyond what is necessary for the provision of service. The AMA emphasizes, for example, that, "a patient *expects* to have his or her privacy respected by the physician and should not be disappointed."[28]

[28] Emphasis added. *Patient Confidentiality*, AMERICAN MEDICAL ASSOCIATION, at http://www.ama-assn.org/ama/pub/physician- resources/legal-topics/patient-physician-relationship-topics/patient- confidentiality.page (Clarifying as well that information disclosed to a physician during the course of the patient-physician relationship is "confidential to the utmost degree," that the physician's duty to maintain confidentiality means that "a physician may not disclose any medical information revealed by a patient or discovered by a physician in connection with the treatment of a patient," and that the purpose of this ethical duty "to allow the patient to feel free to make a full and frank disclosure of information to the physician.").

In the modern commercial wellness and fitness context, in contrast, health information flows are multi-directional, multi-purpose, and are not subject to well-established norms regarding data use or distribution. Without fuss or friction, Fitbit users can easily opt to make broad swaths of health information available to friends or the general public by adjusting and handful of privacy settings on their user portals; they can automatically broadcast fitness status updates to hundreds of followers on Twitter, Facebook, or WordPress; and they can make still more information available to medical professionals, coaches, personal trainers, or others by publishing directly to Microsoft HealthVault. Self-tracking companies can share user information with business associates, data brokers, marketers, insurance plans, employers, or even law enforcement, subject only to self-directed, self-imposed restrictions on the information flow practices decided internally and spelled out to users, often opaquely, in privacy policies. And once information has reached second and third parties, there is very often no way to predict where it will land.

In the realm of health, unconstrained information flows can be particularly perilous. Criminals may have interest in self-tracking data to determine whether a person is at home or currently jogging on a particular trail through the woods. The apps MapMyRun and Endomondo, for example, use a smart phone's GPS capability to track running routes in real time; users can broadcast their exact whereabouts to Facebook and Twitter followers, or the general public. Police may want to establish or confirm residence at an address at a certain critical time. Advertisers will find it valuable to know which brands of food people eat, and how much and how often. The service MyFitnessPal enables users to quickly scan food package barcodes with their smart phone apps; its database of two million food items supports a database of the detailed eating habits (including brand, time of day, and portion size) of some thirty million users. The service will be adding food served on the University of California, San Francisco Medical Center's campuses, and has recently launched a private API allowing syncing with Fitbit, and other companies, including Bodymedia, runtastic, and Endomondo.[29] Employers may base

[29] Natasha Lomas, *MyFitnessPal Adds UCSF Campus Food To Its Database As "Corporate Wellness" Partner*, TechCrunch, Jan. 22, 2013, at http://techcrunch.com/2013/01/22/myfitnesspal-adds-ucsf-campus-food-to-its-database-as-corporate-wellness-partner/

hiring, firing, and other practices on employees health: It is Fitbit's current practice to sell users' aggregate health data to some employers[30] on an opt-in basis as part of corporate wellness sharing partner programs. Enticing employers to "decrease sick leave days, decrease healthcare costs, and increase employee productivity," corporate sharing alerts companies to employee activity data at a population level: Woody Scal, Fitbit's chief revenue officer, explains that "Companies can see how many of the devices they've given out have actually been activated. How many are being used? How is it actually changing employee behavior?" Scal also said, in December, 2012, that Fitbit is working with an insurance company to track whether employees who use Fitbit devices visit their doctors less frequently. "This [finding]," Scal says, "would be the holy grail for a product like this."[31]

Insurance companies are particularly active in the self-quantification space, in some cases partnering with existing services, and in other cases creating their own self-tracking apps so that customers may upload information directly. Aetna, for example, recently launched a smart phone app called CarePass that gives consumers individualized suggestions for how to achieve personal health goals (such as "fitting into your jeans") by integrating data from multiple wearable tracking devices and location mapping apps[32] with individualized patient information about doctor visits, prescriptions, blood pressure and cholesterol records. This tool also includes APIs that allow individuals to grant doctors and other app developers access to their data. Aetna's consumer platform vice president disclosed in June that CarePass will also have a portal that allows employers to gain access to anonymous, aggregate data about their employees as a way to reduce health care costs.

[30] Per Fitbit's website: asurion, Autodesk, Cerner, Pega, practice fusion, and Tokyo Electron. http://www.fitbit.com/product/corporate-solutions, last accessed Aug. 15, 2013.

[31] Aarti Shahani, *Who Could Be Watching You Watching Your Figure? Your Boss*, All Tech Considered, Dec. 26, 2012, at http://www.npr.org/blogs/alltechconsidered/2012/12/26/167970303/who-could-be-watching-you-watching-your-figure-your-boss.

[32] Carepass's full list of partners at launch is MapMyFitness, LoseIt, RunKeeper, Fooducate, Jawbone, Fitbit, fatsecret, Withings, breathresearch (makers of MyBreath), Zipongo, BodyMedia, Active, Goodchime!, MoxieFit, Passage, FitSync, FitBug, BettrLife, Thryve, SparkPeople, HealthSpark, NetPulse, Earndit, FoodEssentials, Personal.com, Healthline, and GoodRx. Jonah Comstock, *Aetna Carepass is No Longer Just for Developers*, MobiHealth News, June 18, 2013, at
http://mobihealthnews.com/23103/aetna-carepass-is-no-longer-just-for-developers/

Not only do these information flows go far beyond what the ordinary health self-tracking user would expect, they carry great potential for practical harm, such as increased rates, loss of benefits, or the dignitary effrontery of having one's every move watched and analyzed—for purposes that are not currently understood, and that may expand in the future. In a recent blog post, insurance consultant Mike Allen contemplates a scenario in which a disability challenge by an employer or insurance company might be more difficult to defend if a smart pedometer had recorded fitness data. *"Let's take a 50 year old truck driver with a severe back strain. Complicating his treatment, he also suffers from obesity and a heart condition which can significantly lengthen expected return-to-work pathways and increase medical costs. Using low-cost apps loaded onto his iPhone, the trucker can watch and then perform stretching exercises prescribed by his physical therapist. A wristband device can monitor his movements to make sure he is meeting agreed-upon activity levels and not spending all day in bed. Finally, he can use an iPhone-based biofeedback trainer to lower his stress levels and blood pressure readings. While this example is hypothetical, mHealth applications which perform these functions and many more are available to workers' compensation players today. In the near future the truck driver's mHealth devices will update his Electronic Health Record (EHR) in real time, integrate with claims, case management and other workflows and notify his health team of problems."*[33] From the perspective of an insurance consultant, these uses of consumer-oriented mobile health tools are a great boon to cost savings. From the perspective of the surveilled truck driver, they may cast a chilling pall on his freedom of movement and association.

In some cases, tracking can even extend to the next generation of users. The Glow app, a free tool that tracks users' sexual activity, basal body temperature, emotional health, and other very personal menstrual cycle markers (such as cervical mucus texture), predicts days in which a woman is most likely to be fertile and sends her, and her partner, daily reminders and suggestions to assist in the quest to conceive. Glow First, an optional add-

[33] Mike Allen, *How Mobile Health is Revolutionizing Medicine!*, TECH TALK FOR WORKERS' COMP, Feb. 4, 2013, at https://michaelgallen.wordpress.com/2013/02/04/how-mobile-health-is-revolutionizing-medicine/.

on program that co-founders, former Google and PayPal executives, refer to as a community for "crowdfunding babies," allows some women to pay $50 per month into a collective fund: Should conception not occur within 10 months of consistent tracking, a member will be eligible to draw from the fund pool to help offset the costs of infertility treatment; funds will go directly to the fertility clinic of the woman's choice. Because fertility treatments typically run families into tens of thousands of dollars, the incentive to participate in the Glow First program is high. In return, the founders get a great deal of information about women's body and behavioral habits and relationships with their partners; they also get a head start on tracking any children are conceived. This intriguing information sharing model combines a complexity of elements: health advice, social support, financial remuneration, and even public health research. "Once we have a few hundred thousand data points," explains one of the co-founders, "we'll know a lot more about infertility."[34]

Insufficient Disclosures

As a practical matter, users are likely unaware of the extent to which their data can be shared with third parties because companies do not provide full descriptions of data flows in privacy policies, and because privacy settings are insufficiently mapped to collection settings. Data is often transferred first to service providers in the cloud and then displayed to users on a provider dashboard; additionally, partner relationships between app-linked devices and other health monitoring services lead to data being combined from multiple sources and made available on multiple services, a proliferation that is difficult for users to manage. Further, users may grant access authorization to sites incrementally, even forgetting to revoke authorization once they have lost interest and moved on; thus, they may not be aware of the total amount of information they are sharing over time, and with whom.[35]

[34] Quentin Hardy, Happy Birth Data! A New App Tracks Fertility, New York Times Bits, Aug. 8, 2013, at http://bits.blogs.nytimes.com/2013/08/08/happy-birth-data-a-new-app-tracks-fertility/?_r=0.

[35] Thanks to Vincent Toubiana for flagging many of these issues in conversation, and for providing an advance draft of an unpublished report, *Survey on Privacy Threats Posed by Smart Sensors*, EIT ICT Labs, Jan 30, 2013.

In other cases, consumers are given inadequate tools with which to make responsible choices about information disclosures. The fertility app Glow, for example, states in all capital letters in its privacy policy that, "WE DON'T SELL OR RENT YOUR PERSONAL INFORMATION TO THIRD PARTIES." Although this attention-grabbing text is reassuring, smaller print in the following paragraph clarifies that "We share your personal information with employees, affiliates, vendors, partners, and third parties, as required to offer the ServiceS" [sic]. Further down on the page, it is additionally revealed that the company shares "your personal information…to market products and services to you" and that it shares user "transactional information" and "experiences" with affiliates. Thus, although the company may not "sell or rent" consumer data, neither does it appear to place many actual limits on "sharing" with a large number of third parties, for vaguely described purposes. "Personal information," in this case, is incompletely defined a "your name, address, phone number, third party application IDs, and other 'similar information.'" "Transactional information" and "experiences" are undefined.

Security Risks

Health and wellness devices are well known among security researchers to lack features that would protect users from harm. A recent review of 43 health and wellness apps by the Privacy Rights Clearinghouse (PRC) revealed that many apps send personally identifiable and other sensitive information, including disease and pharmaceutical search terms, to third parties unencrypted, and in the clear.[36] Security concerns were such that PRC authored a separate technical report for health and fitness app developers, advising them to always use HTTPS, to fully anonymized all data shared with third party analytics services, to encrypt all network communications with SSL, to never send user information in clear text, to salt and hash all passwords before sending or storing, and to not expose private data in URLs. The report warns that *none* of the apps PRC analyzed takes all of these precautions.[37]

[36] Linda Ackerman, *Mobile Health and Fitness Applications and Information Privacy, Report to the California Consumer Protection Foundation*, PRIVACY RIGHTS CLEARINGHOUSE, July 15, 2013, at https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf.

[37] Craig Michael Lie Njie, *Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications*, PRIVACY RIGHTS CLEARINGHOUSE, at http://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf.

In a separate blog post, security researcher qDot (Kyle Machulis) describes Fitbit security flaws.[38] Any Fitbit tracking device will synch with any base station or computer with a wireless sync dongle within range, and automatically upload stored data to the user's account. Fitbit considers this to be a feature, not a bug—a convenience to its users made possible by virtue of the association between the tracker's unique serial number and user ID on Fitbit.com. In practice, however, this means that anyone with these two pieces of information could gain access to a user's Fitbit account, and possibly to other self-monitoring service accounts that the user links to through Fitbit. As Machulis notes, "This is an incredibly easy system to spoof. I could walk around with a netbook and a [F]itbit base station in my backpack, gather serial numbers at a public Meetup, then have all the account information I wanted."

Erosion of Social Norms

Ethical issues associated with health self-monitoring also abound: Scott Peppet[39] and Frank Pasquale have keyed in on an interesting intersection between self-quantification, privacy, and social norms, noting that we may soon all be expected to track, else be assumed to be hiding bad behavior. *Unraveling* is a term they use to describe the phenomenon whereby the disclosure of personal information for economic gain becomes so inexpensive, easy, and common that those who do NOT disclose are assumed to be withholding negative information, and therefore stigmatized and penalized. Peppet asserts that unraveling presents a threat to privacy because "when a few have the ability and incentive to disclose, all may ultimately be forced to do so." For example, if a driver can get a lower insurance premium by agreeing to a tracking device being placed on his car, a driver who refuses to be tracked may be assumed by the insurance company to be signaling unsafe driving habits, and expect at some point to face price discrimination as a result of non-participation. Pasquale advises the Office of the National Coordinator for Health Information Technology that, "*[Self-quantification] may seem like an odd habit of*

[38] Kyle Machulis, *Fitbit and Security, or Lack Thereof*, OPENYOU, April 18, 2011, at http://www.openyou.org/2011/04/18/fitbit-and-security-or-lack-thereof/.

[39] *See* Scott Peppet, *Unraveling Privacy: The Personal Prospectus & The Threat of a Full Disclosure*, NORTHWESTERN UNIVERSITY LAW REVIEW (2011), pg. 4, available at https://www.law.northwestern.edu/lawreview/v105/n3/1153/LR105n3Peppet.pdf.

nerds right now, but I promise that as wellness programs and other sorts of benefits become more popular it's not going to be easy to avoid them. People are going to wonder why aren't you part of the quantified-self movement? What are you trying to hide? Are you trying to hide your cholesterol level from us? I think that even though they seem that they are the vanguard now, this privacy phenomenon called unraveling can very quickly lead [to] a tipping point where everyone feels not just that it's helpful but that they need to be part of these things. [40]

III. Existing Medical Legal Protections are Insufficient to Protect Consumer Privacy in the Mobile Health Ecosystem

A patchwork of federal rules provides little guidance on privacy protections specifically tailored to the mobile health self-tracking ecosystem. At present, there is no federal privacy law in the U.S. that applies specifically to commercially available mobile health and wellness tools intended for use by consumers. As explained in more detail below, the Health Insurance Portability and Accountability Act (HIPAA), the federal health privacy law promulgated and enforced by offices within the Department of Health and Human Services (HHS), does not typically apply to off-the-shelf health sensors and apps used by individuals to track and store their own data with commercial services. Anticipated Food and Drug Administration (FDA) regulations regarding the safety and security of mobile medical apps will likely deliberately exclude commercial fitness and wellness apps from oversight. It remains to be seen whether coordinated efforts underway by the Office of the National Coordinator of Health Information Technology (ONC), the FDA, and the Federal Communications Commission (FCC) to create a comprehensive, risk-based regulatory framework pertaining to health information technology, will aim to protect individuals' safety in health devices and apps that are not considered to be strictly *medical* in nature. Finally, although the Federal Trade Commission (FTC) likely has general jurisdiction under Section Five of the FTC Act to pursue actions against mobile health and wellness entities engaging in "unfair and deceptive trade practices," such as,

[40] U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Roundtable: Personal Health Records, Understanding the Evolving Landscape, Dec. 3 2010, available at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__personal_health_records_–_phr_roundtable/3169.

for example, failing to adopt, disclose, or adhere to reasonable privacy and security practices, these protections do not directly address the needs of consumers in the context of health information flows.

HIPAA/HITECH. In traditional medical contexts, the privacy of individuals' personally identifiable health information is enforced by the HIPAA privacy rule, promulgated in 1996 by the U.S. Department of Health and Human Services, and updated in January 2013.[41] HIPAA implements a version of the Fair Information Practice Principles (FIPPs)[42] and sets a floor for the protection of identifiable health information which the States or covered entities (as a matter of organizational policy) are free to expand. HITECH expands privacy protections in electronic data held by HIPAA covered entities.[43]

In most canonical, consumer-oriented use cases, sensors and apps will not fall under the purview of HIPAA. First, HIPAA only applies to "covered entities," and their business associates. Covered entities are (a) health care providers[44] who transmit health information electronically in connection with a transaction for which the Secretary has adopted a standard, (b) health plans, and (c) health care clearinghouses.[45] Business associates of covered entities are entities with agreements in place specifying that they manage "protected health information" on that entity's behalf. Second, HIPAA applies

[41] Modifications to the HIPAA Privacy, Security, Enforcement, and
Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules" (Omnibus Rule), 78 Fed. Reg. 5566, Jan. 25, 2013, at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/html/2013-01073.htm.

[42] In adopting the rule, HHS said, "This final rule establishes, for the first time, a set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care." Department of Health and Human Services, Final Rule, Standards for Privacy of Individually Identifiable Health Information, 65 Federal Register 82462, 82464, Dec. 28, 2000, at http://www.gpo.gov/fdsys/pkg/FR-2000-12- 28/pdf/00-32678.pdf.

[43] The rule also expands the definition of business associates to encompass patient safety organizations, health information organizations, e-prescribing gateways, persons that provide data transmission services or facilitate access to health records, and vendors of personal health records provided on behalf of covered entities, 45 C.F.R. § 160.1, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

[44] *Health care provider* means a provider of services (as defined in section 1861(u) of 42 U.S.C. 1395x), a provider of medical or health services (as defined in section 1861(s) of 42 U.S.C. 1395x), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. Definitions available at: http://www.ssa.gov/OP_Home/ssact/title18/1861.htm; 42 USC 1861(s), available at http://www.ssa.gov/OP_Home/ssact/title18/1861.htm.

[45] *Business associates* are persons or entities that create, receive, maintain, or transmit PHI on behalf of, or in the provision of certain services to, a covered entity.

only to "protected health information," which is information relating to an individual's physical or mental health, health care service, or health care service payment that individually identifies that patient, and that is *created or received by* a health care provider, health plan, employer, or health care clearinghouse. Thus, information is protected by HIPAA only if it is PHI, and information is PHI only if it is personally identifiable and is also held by a HIPAA covered entity.

Here, most mobile sensors or apps used by consumers or patients will not fall under HIPAA. First, entities holding the information—individuals tracking their own metrics, or sensor or app developers or companies— are not HIPAA covered entities. Health care providers, for example, are providers of medical or health services, and typically include doctors, dentists, hospitals, skilled nursing facilities, comprehensive outpatient rehabilitation facilities, home health agencies, hospice programs, and the like.[46] Health plans are individual and group plans that provide or pay the cost of medical care, such as medical, dental, and vision insurance providers, Medicare and Medicaid, HMOs, and some company health plans. [47] Health care clearinghouses are entities like billing services and repricing companies. Business associates include, for example, pharmacy benefits managers and health information exchange organizations.

Second, the information in question, although often personally identifiable, is not protected health information as defined in the Rule, by virtue of not being held by a HIPAA covered entity. Thus, even if insurance plans provide their customers with apps for tracking fitness and weight and other biomarkers, the app is not subject to HIPAA if the data is stored by the user, for example, on his or her own smart phone. However, if an individual user transmits PHI to a covered entity, or to a business associate of a covered entity, then the information is subject to HIPAA once it is received by that entity. Thus, a health care plan that offers its enrollees a health tracking app and stores those individuals' self-generated health information on its own servers may well be subject to the Rule.

[46] 42 U.S.C. 1395x, § u.

[47] Summary of the HIPAA Privacy Rule, Health Information Privacy, Department of Health and Human Services, at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.

If HIPAA does apply, individuals are granted some affirmative rights over their data, and some restrictions are placed on the distribution of that data to third parties. For example, Individuals are entitled to receive electronic copies of their health information, and they can restrict treatment disclosures to health plan if they pay out of pocket in full. They also have a right to expect that entities will employ appropriate security safeguards, including encryption and other protections against interception, user authentication, and systems for recording when a patient's or enrollee's protected health information has been accessed. The Privacy Rule also prohibits covered health care providers and health plans from selling protected health information to third parties, such as for the third party's own marketing activities, without authorization. However, wide carve-outs do permit covered entities to disclose PHI to third parties without a patient's consent for a number of purposes, including treatment, payment, or health care operations; in emergencies; or for the public's interest and benefit, such as for serious threats to health or safety, or to report domestic violence, for research purposes, and as authorized by workers compensation. A covered entity can even share protected health information with telemarketers if it has entered into a business associate relationship with the telemarketer for the purpose of making a communication that is not marketing, "such as to inform individuals about the covered entity's own goods or services."

In sum, in most of the situations that consumers find themselves in today, including buying a fitness tracker at a local retailer, or downloading a health or fitness app for personal use, HIPAA is unlikely to apply. Even if it does, HIPAA coverage simply does not ensure that individuals have the opportunity to control most uses or disclosures of their health information.

FDA. To date, FDA has not promulgated a policy covering the regulation of software applications intended for use on mobile platforms. According to draft guidance issued in June 2011, as well as FDA Congressional testimony before the House Energy and

Commerce Committee in March 2013,[48] FDA plans to take a narrowly tailored approach to mobile health app regulation.[49] Regulatory oversight will be focused on only a subset of apps that both meet the definition of a medical device and (1) are used as an accessory to a "regulated medical device" or (2) transform a mobile platform into a "regulated medical device." The FDA explicitly does *not* consider general health and wellness apps to be mobile *medical* apps for purposes of regulatory oversight. Specifically "*mobile apps that are solely used to log, record, track, evaluate, or make decisions or suggestions related to developing or maintaining general health and wellness [if] [s]uch decisions, suggestions, or recommendations are not intended for curing, treating, seeking treatment for mitigating, or diagnosing a specific disease, disorder, patient state, or any specific, identifiable health condition*" will not be regulated. Examples include dietary tracking logs, appointment reminders, dietary suggestions based on a calorie counter, posture suggestions, exercise suggestions, or similar decision tools that generally relate to a healthy lifestyle and wellness.[50] Moreover, since app stores themselves are not intended for medical purposes, they will not be regulated.

FDASIA. In recent months, lobbying efforts have been underway to move some of FDA's mobile health oversight to ONC, and to urge FDA to refrain from issuing any regulations in advance of a report to be issued in January 2014 by a joint regulatory task force comprising personnel from FDA, ONC, and FCC. Under section 618 of the Food and Drug Administration Safety and Innovation Act (FDASIA,)[51] the ONC, FDA, and FCC have been charged by Congress with developing a risk-based regulatory framework for health information technology that would "promote innovation, protect patient safety,

[48] Press Release, *Committee Announces Three Day Hearing Series on Health Information Technology to Explore Potential Regulations and Taxes on Smartphones, Tablets and Mobile Apps*, ENERGY AND COMMERCE COMMITTEE, March 12, 2013, at http://energycommerce.house.gov/press-release/committee-announces-three-day-hearing-series-health-information-technology

[49] Under Section 201(h) of the Federal Food Drug & Cosmetic Act (FDCA), a *medical device* is defined in part as an instrument, machine or other apparatus which is (i) ''intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease,'' or (ii) ''intended to affect the structure or any function of the body.'' FDA, *Is the Product A Medical Device*?, at http://www.fda.gov/medicaldevices/deviceregulationandguidance/overview/classifyyourdevice/ucm051512.htm.

[50] *Draft Guidance for Industry and Food and Drug Administration Staff, Mobile Medical Applications*, FDA, July 21, 2011, pg. 11, at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

[51] http://www.gpo.gov/fdsys/pkg/PLAW-112publ144/pdf/PLAW-112publ144.pdf.

and avoid regulatory duplication."[52] Although ONC is actively involved in addressing health privacy and security issues—for example, by organizing a Privacy & Security Tiger Team workgroup, it remains to be seen whether the protection of patient safety will be interpreted more broadly to include protecting individuals' privacy in health information technology, such as sensors and mobile apps, that are not considered *medical* by FDA.

FTC. In the absence of specific legal protections for the highly revelatory data collected by third-party providers of mobile health tools, consumers are in the position of relying on firms' self-regulatory practices, communicated to them through long-discredited notice and consent styled privacy policies and backstopped primarily by the Federal Trade Commission's (FTC) unfair or deceptive trade practices oversight and contract and tort law. FTC has emphasized the importance of data privacy in mobile applications more generally,[53] urging app developers to "get it right from the start," by curbing the amount of information they collect, storing that information securely, limiting access to a need-to-know basis, and safely disposing of it when no longer needed. FTC also counsels developers to be transparent about data practices, to offer users easy-to-find tools that allow for simple adjustments of information collection and sharing practices, and to honor promises made in privacy policies. These principles are clearly applicable to mHealth apps. Although the FTC has not specifically aimed guidance at the mobile health sector, it has barred two health app developers from making unsubstantiated health-related claims without competent and reliable scientific evidence.[54]

Recently, FTC enforcement authority has been invoked by the Administration in its Privacy Bill of Rights. Additionally, in February 2012 the Commission issued a Privacy Report calling on companies to introduce privacy into the design of products at every build stage, to incorporate greater transparency about the collection and use of

[52] *FDASIA*, Health IT Policy Committee, HEALTHIT.GOV, at http://www.healthit.gov/policy-researchers-implementers/federal-advisory-committees-facas/fdasia.

[53] *Marketing Your Mobile App: Get it Right from the Start*, FCC at http://business.ftc.gov/documents/bus81-marketing-your-mobile-app.

[54] *''Acne Cure'' Mobile App Marketers Will Drop Baseless Claims Under FTC Settlements*, FTC, Sept. 8, 2011, at http://ftc.gov/opa/2011/09/acnecure.shtm.

consumers' information, and to provide consumers with choices where business practices are not "consistent with the context of a transaction or a consumer's relationship with the business."[55]

IV. Privacy Vulnerabilities Emerging from the Fitbit Study

Background

As discussed above, in 2012, the Obama Administration unveiled a four-part framework for creating consumer privacy rights in commercial sectors not currently subject to Federal data privacy laws. The framework originated with the release of a Consumer Privacy Bill of Rights, a FIPPs-based set of principles holding that consumers have a number of rights that, in turn, impose obligations on companies. These include the right: (1) to exercise control over what personal data companies collect from them and how they use it; (2) to [have] easily understandable and accessible information about privacy and security practices; (3) to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data; (4) to [obtain] secure and responsible handling of personal data; (5) to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate; to [expect] reasonable limits on the personal data that companies collect and retain; and to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

The third principle, Respect for Context, requires companies to consider what consumers are likely to understand about their data practices based on the products and services they offer, how the companies themselves explain the roles of personal data in delivering them, research on consumers' attitudes and understandings, and feedback from consumers. Context should also "help to determine which personal data uses are likely to raise the greatest consumer privacy concerns. The company-to-consumer relationship

[55] Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers, FTC, Mar. 2012, available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

should guide companies' decisions about which uses of personal data they will make most prominent in privacy notices."

Method

Study methodology is described more fully in a report in progress.[56] To summarize: twenty-one interviews have been conducted: sixteen in the New York City metropolitan region and five in the San Francisco Bay Area. Each participant was interviewed during a single, two-hour, audio-recorded session at a mutually convenient location. Each session consisted of: (1) a one-on-one conversation that adhered closely to a structured qualitative interview script, including the administration of a privacy attitudes, behaviors, and knowledge questionnaire; and (2) the administration of a card-sorting exercise. Participants were paid $40 per hour.

Participant Recruitment. A convenience sample was obtained by placing an advertisement within two Fitbit.com community groups, "!New York FitBit!" and "!San Francisco Bay Area!". These groups are viewable to the public; they have approximately 2,000 members each. Interested viewers of the ad contacted me directly. Participants were screened to ensure that they met demographic criteria[57] and understood and agreed with the parameters of the study. A first round of interviews was conducted over a two-week period from March 5 to March 15, 2013. Two follow-up ads were subsequently placed, adhering closely to the text of the original, within the "Anyone from Manhattan" discussion topic within the !New York FitBit! Group. I conducted a second round of interviews from April 6 through April 18, 2013, and a third round during July 2013. Interviews are ongoing.

Interview. Participants gave informed consent and completed a brief demographic questionnaire before beginning the study. Fitbit participants were engaged in structured conversation to learn more about motives for using a health tracker, use routines, positive and negative experiences with the device and the Fitbit community, and expectations and

[56] Heather Patterson, *Individuals want granular privacy control over health information in mobile health devices*, Manuscript In Progress.

[57] Fitbit users 18 years or older and residing in the NYC or SF Bay Areas

preferences regarding information flows. The primary goal was to develop a fuller contextual understanding of participants' engagement with the Fitbit, both as an omnipresent tracking device and as an information-sharing ecosystem. Interviews adhered closely to a prepared script; this script alternates between two question-and-answer periods, one interactive exercise, and the administration of a questionnaire, described below:

- During the first question-and-answer period, participants were invited to explain their initial and ongoing motivations for acquiring and using a Fitbit tracker, including describing their daily information collection and self-monitoring behaviors, and any perceived changed approaches to their health and wellness behaviors they experience while using the device.

- During the interactive portion of the interview, participants were asked to create a hand-written list, from memory, of all information they currently collect and record with the Fitbit tracker and on Fitbit.com, and all recipients of this information, both online and offline. Participants were then asked to sign in to their Fitbit.com accounts, to guide me through their Fitbit.com information collection and sharing settings, and to make note of any discrepancies between their actual and self-reported information management practices.

- During the second question-and-answer period, participants were asked to give their general impressions of Fitbit's business model, information security practices, and trustworthiness, including any obligations the company may have under the law to protect user information privacy and security. They were then asked to provide similar impressions of their own medical care providers' information-management practices and trustworthiness. During this portion of the interview participants also generated a list, typically orally, of information collected in the context of a routine visit to their health care providers' office, as well as likely recipients of this clinically generated health information.

.

Card Sort. After answering questions in the structured interview guide and completing the information-sharing questionnaire, participants completed a card-sort task designed to assess their preferences for sharing a wide range of wellness and health information types with a variety of potential recipients. Information items were printed on white index card stock; information recipients were represented as labeled manila file folders in a portable file box. Participants indicated which information items they would feel comfortable sharing with which recipients by placing cards in file folders, and explaining aloud their reasoning.

Caveat. A number of specific vulnerabilities and sources of concern about user privacy emerged over the course of my conversations with fitness self-trackers. However, I caution that the formal interviews that gave rise to these observations were conducted with a relatively small number of users of one self-tracking tool, and thus results may not be properly generalizable to the larger population of health self-trackers. Rather, these observations may most usefully serve as starting points for further considered discussion, and for designing larger scale surveys or experiments aimed at exploring privacy preferences and vulnerabilities in the consumer-oriented mobile health space.

Findings

Participants in this study…

(1) …are vulnerable to persistent health tracking because they adopt a "put it on and never remove it" device wearing strategy. Participants in this study spoke of the Fitbit tracker as a personal object that has become a fully integrated part of the body and the daily routines—an intimate device to be donned first thing in the morning, worn all day and night, and monitored frequently. Physical design attributes, such as waterproof wristbands or clips that allow devices to be worn discreetly, under clothing, promote ubiquitous usage: One user, very typical in his habits, explained that, "I pretty much wear [the Fitbit] all the time. I'll put it on as part of my routine getting ready in the morning. I'll hook it into my pants, and I'll wear it throughout the day until I get back home. If I do go out (or if I'm going to go down and do laundry, 'cause there's stairs [down to the washing machine], and that counts as a flight), I'll make sure I wear it. Most of the time I wear it when I asleep. [Whenever] there is an opportunity to log stairs or miles or steps or whatever, I'm going to wear it." Another woman said, "I only take it off to shower. I have it on at night on an armband and I switch it on before I fall sleep and I switch it off when I wake up and I carry it around with me all the time...I wear it everywhere; I don't really ever not wear it." A third, who owns a waterproof wristband model, literally never removes it. "[I wear it] every day. I don't take it off for anything...It's waterproof, so I wear it in the shower…So I haven't taken it off at all." A fourth reported, "It's such a part of me now. For some reason too because of where I wear it, I think it's an intimate relationship. That sounds really weird, but I wear it on my bra, so I feel really connected to it. I don't think about it most of the time because I can't feel it…."

Motivational messages sent to the sensor or the associated smart phone app, such as personalized encouragement ("Hi Heather!"; "Walk me!"), or an image of a flower that grows and shrinks with activity, encourage continued engagement and use, such that only two of the twenty-one people I have spoken with reported that they would not turn around to retrieve the device if they accidentally left it at home that day. "The second time that I got to 10 thousand [steps] was this past Friday and I had a weird day…but at the end of the day, it was probably like 11:40[pm] and I got a [message] on my phone saying like, 'You have three hundred seventy something steps to go.' I was like, 'Oh, really?' <laughs>. And I was like pacing back and forth and around my apartment. My cat probably thought I was insane. I was like stepping over her <laughs>." Typically, people reported that they would turn back if they were two blocks from home if on foot, or two miles from home if by car. "I think that I would feel like something's missing, and I'd constantly check the app and then realize, "Wait, I don't have it on me right now." I would definitely feel naked."

Few people recognized possible harms associated with ubiquitous tracking, although several pointed out their friends' activity to me, and made on-the-spot inferences about whether particular friends were on vacation, feeling under the weather, running a marathon, or not yet at work that day. Others acknowledged the possibility of being tracked by friends, and accidentally 'caught out' if they were trying to keep their behavior private: "If I ever told my girlfriend like 'Hey, I'm going to bed now,' and then she looked [at my stats] and like, two hours later 5000 steps were added [to my step count], she'd be like, 'You said you were going to bed. Where'd you get the steps?' That would be odd and even creepy."

No one flagged the possibility of behavioral and location integration through self-tracking sensors and cell phone apps. However, many people I spoke with indicated that they would be uncomfortable if their fitness sensor contained a geo-locative GPS tracker, explaining that this would too invasive, that they didn't want one company having too much information about them, and that they envisioned security dangers. Talking about the possibility of being able to share favorite hiking or biking paths with tracking services, one woman said, "Now, this is more like the GPS function that some of the trackers have, which is always interesting…Somebody could stalk you. Somebody could see that every Tuesday you go on a certain run. With a public profile they could go, 'This is where I'll find you.'" A man reported that he would enjoy being able to use his Fitbit to track geolocation so long as that feature could be controlled with a simple "off" switch that gave him easy control over being tracked. Another woman said, "I don't think I'd use [the Fitbit if it had a GPS tracker], honestly, just because I-- that's just-- that's too invasive. <laughs> And if it's information like-- if it's something like Fitbit, where people can see my profile and stuff like that, I don't want them to know where I'm at all the time, and keep tabs on me, and-- because I do have the tendency to be like, 'I'm unavailable right now.' And if they're like, 'I know you're down the block,' I would be so upset, because I like my private time, and I don't need everybody to just be on top of me. And that's really scary if somebody knows where you are. They could stalk you and stuff."

(1) Suggestions regarding ubiquitous usage:

- Explain to users, before they begin tracking, how frequency of device usage is associated with frequency and comprehensiveness of health data collection. For example, tell users how often individual activities and behaviors are recorded, e.g., minute-by-minute, hour-by-hour, and which parties have access to their information, at which degree of granularity.

- Explain to users, before they download or open an app, whether the app will track the user's location, as with run tracking services, and whether location information can (or will be) combined with other health behavioral information.

- Educate users about the sensitivity of the tracking sensors within the device or app, including altimeters, three-axis accelerometers, and methods of tracking physical location, and explain whether and how accurately those sensors can support inferences about user behavior, such as sexual activity, particularly when combined with information about time of day and duration.

- Consider incorporating a simple, user-controlled Do Not Track feature into sensors and apps, whereby a device button press or clock setting halts information tracking or automatically stores recorded information as "private" to the user during that time window.

Participants in this study…

(2) …underestimate the amount of information they share with Fitbit and other health tracking services. Broadly, sensor and app services serve as repositories of many of the same types of health information that individuals are accustomed to sharing with their doctors, but lack the traditional cues and privacy protections of the medical office. This contextual ambiguity appears to leave users uniquely vulnerable to uncontrolled, large-scale information disclosures: On the one hand, because self-monitoring tools are *health*-oriented, individuals I spoke with were likely to be both scrupulously truthful when supplying details of their anatomical and physiological states to sensor and app developers upon enrollment. Participants had little incentive to obscure true personal health attributes, because their ultimate goal was to receive personalized health guidance. But because individuals conceive of the Fitbit primarily as health-oriented *lifestyle* tools rather than medical tools, they were likely to be less scrupulous about sharing large quantities of information, or of taking advantage of limited opportunities to keep information private, or to educate themselves about back-end information flows.

When I asked participants to make a list, from memory, of information they log on the Fitbit device or record on Fitbit, com, most (correctly) reported tracking step counts, calories burned, distance traveled, and flights of stairs climbed; many also report uploading a picture. Nearly half also use a partner app for logging food—typically, MyFitnessPal or LoseIt!—they noted this and explained that their food stats auto-populate Fitbit food and calorie fields. However, when we subsequently logged into the participant's Fitbit.com accounts together, we discovered that many had failed to list sleep duration and quality as a recorded metric, and that most had not reported giving Fitbit their account information—including real names, date of birth, email address, zip code, city, state, and country, gender, height, and "about me" descriptions.

In some cases users appeared not to know which pieces of information were optional and which were required, erring on the side of completeness. "Well primarily what I was thinking when I was completing the profile is, "Okay, they are asking for this information, why do they need it? Is it actually going to impact the data that I gather?" Some people explained that they provided complete information because they want accurate fitness recommendations, noted above; others viewed accuracy and completeness of disclosure as a hedge against allegations of fraud, should they need to contact the company with a request to fix or replace a broken device. "I like to put my real name on things like this…because in the event it's ever broken or damaged I feel like my name is there, as opposed to trying to enter it last minute and there's a suspicion of, 'Well, your name was just entered the day it broke," so it's like 'No, dude. It's been mine the entire time.'"

(2) Suggestions regarding information sharing:

- Clearly delineate between information that is optionally provided, and information that is required for provision of service and for warranty or other service communications.

- Be particularly clear about explaining which pieces of information will improve (or diminish) accuracy of health feedback.

- Because small fitness trackers get lost or damaged frequently, explain to users how much demographic information is necessary at the registration stage to establish ownership, should users later need to contact the company about a replacement device

- On a single page, display for users all of the information held about him/her, both from the fitness service in question and from other linked services if possible, including the time span and duration over which that information is logged and stored.

Participants in this study…

(3) …are often uncertain about how to operationalize their health information sharing preferences. Many users claimed to have adjusted their privacy settings online, but were surprised, when we visited their privacy settings page together, to find that they had been sharing some types of information with the general public. It was common, in fact, for the people I interviewed to believe that making information "public" meant that they were sharing information with all registered Fitbit users (regardless of their "friendship" relationship with those users), rather than all Internet users, writ large. It was also common for people to not remember what their sharing settings were, or to be unable to explain their rationale in selecting and maintaining those settings. Over half of individuals I spoke with adjusted their privacy settings during the course of our interview. A common response to viewing privacy pages was, "No, I haven't changed these [settings]. Wait, I take that back…I have." [On reviewing one's own settings]: "I'm surprised at how arbitrary these seem. Why did I make these decisions?"

Some people complained of a lack of 1:1 correspondence between the labels describing logged information types on the user dashboard, where users are accustomed to viewing their own fitness achievements and, and labels used to describe logged information in the privacy settings. Others felt that their information sharing options were insufficiently granular, or that all information sharing settings should default to private: "Well, I would never do anything all default public. I think that probably the most prudent way that they should structure it is all default private and then people can choose to share." At the time of our interviews, users could not identify ways to view or adjust privacy settings on the smart phone app.

(3) Suggestions regarding privacy settings:

- Make health privacy settings meaningful, granular, easy to find and adjust, and privacy protective.
  - *Meaningful* means that there is a clear correspondence between the types of information collected about users and the representations of those types of information in the privacy settings. For example, the same terms "location" vs. "zip code" should be used in both fields.
  - *Granular* means making individual types of information, e.g., weight, height, age, step count, etc. individually adjustable, rather than combining them into predefined categories, and allowing users to establish personalized recipient categories beyond, e.g., merely "private," "friends," or "public."
  - *Easy to find and adjust* means displaying privacy settings prominently and such that users can make changes quickly, including on the app.
  - *Privacy protective* means arranging data types hierarchically or categorically according to health data sensitivity, and making data distribution "private" or "not shared" by default.
- Explain to users whether "public" means, e.g., that their information is viewable to all registered users of that service, or to everyone online.
- Show users how their dashboards appear to various information recipients, e.g., friends or the public, and allow them to easily make changes, either by adjusting the sharing category of that recipient, or by adjusting the privacy of particular information types.

- Guide users back to their privacy page on a regular basis and prompt them to evaluate their current settings.

Participants in this study…

(4)…do not have a clear understanding of back-end information flows, and deliberately withhold sensitive health information as a hedge against accidental disclosures. Some people I spoke with conceptualized Fitbit and other health and wellness services as neutral and trusted "repositories" for their health information; these individuals had only vague, and typically erroneous, notions of permissible back-end information flows to third parties. "I think of the company as sort of the [storehouse] of my information, less than recipients. I would hope that they're not poring over [my information]. I just think that they're receiving it and storing it for me."

More often, people were skeptical about back-end information flows and deliberately withheld information because of uncertainty about how it will be used, and by whom. These individuals purposefully restricted the amount of information that they logged with Fitbit. For example, a young woman decided to use the service to track her exercise and her food intake, but not her mood or personal reflections because she envisioned Fitbit employees reading her diary entries, or selling her information to third parties. As she explained, "I'm okay with [Fitbit]… seeing I ate, like, Chinese noodles or...an orange or something that I don't care [about], but I don't want…them to read about my personal life. [Y]ou know, it gives information about whether I have allerg[ies] or not and probably [Fitbit] will use it to sell information to pharmaceutical companies or something; that's what I think." A woman flagged potential hiring difficulties as reason not to share health information with Fitbit: "If I were a diabetic, would I enter in my glucose level [on Fitbit]? Probably not. If, let's say, if I were looking for a job or something, and somehow someone had access to that [information] and knew I was diabetic, [it] might impact them hiring me for some reason, right? It's like, 'Okay, we've got two equal candidates, this one is diabetic, I don't know how severe it is, but we're not going to [take the chance and] hire her.'" Another person was concerned about discrimination, generally: “I don’t care if somebody-- if they were to hack into this and they found out how much I ate and how much I walked and how much I weighed, fine. But if someone found out that I had high blood pressure or that I had diabetes and my weight--I mean I’m not overweight…to an extent that I think somebody would discriminate against me, [but] if my weight were at that level, if I [were] obese, I probably wouldn’t want somebody to see it because people might judge me or discriminate against me.”

(4) Suggestions regarding communicating about information flows:

- Because the consequences – real or imagined – of unwanted information flow disclosures are great in the health context, self-tracking companies need to be particularly transparent about which third parties get access to which pieces of information, and under what circumstances.

- Communicate to users, in clearly understandable terms, which granular pieces of their *individual* information will be viewable to Fitbit employees, business associates, and any other third parties, including other apps and fitness services using APIs or companies that might have a particular incentive to purchase health data, such as insurance companies, employers, or pharmaceutical companies.

- Consider adopting visual depictions of data flows, with solid, dotted, or muted lines between information types and recipients, and allow users to make adjustments to their own data flows by clicking on those lines.

- If data will be de-identified, anonymized, aggregated, or otherwise made less traceable to individuals before being made available for viewing or distribution, explain this process, and give concrete “before” and “after” examples, with users’ own data.

- If users can limit the service's information disclosures, tell them how they can do so. For example, if selecting different privacy settings affects data identifability or storage format, explain how, in easily understandable language and at a meaningful time and place, such as *on the privacy settings page* and *as users make those adjustments*.

Participants in this study…

(5)…lack sufficient tools to objectively evaluate health information flow practices, and instead adopt strategies for assessing company trustworthiness that leave them susceptible to bias. The people I spoke with were uncertain about back-end information flows because they do not have a clear, accessible, and understandable source of information. Every participant, save three, reported "never" reading privacy policies, which they consistently dismissed, usually with a scoff, as too long, too complicated, and written "by lawyers, for lawyers." Two remaining participants claim to read privacy policies "sometimes"; one reads them "always." Only this person had read Fitbit's policy in its entirety. One person took issue with the entire concept of privacy polices. He said, "I don't consider 'agreement' to be consent. Legally we're agreeing to it, but who's reading it? I wouldn't feel good even if I 'agreed' to [something]. If it's, like, 'Here's a 20-page privacy policy and [the critical piece of information is] buried in there and I agreed to it, I don't consider that agreeing to it. It's not the same as checking a box that says, 'Yes, I want information from third-party vendors.'"

It was common for people to express this kind of cynicism about privacy notices. At times, people appear to *expect* obfuscation, manipulation, and information leakage. For example:

> **Heather**: Do you typically read privacy policies?
>
> **Kathy:** No. Does anybody? <laughs>
>
> **Heather:** Why don't you?

> **Kathy:** It’s a lot of jargon. It’s way too long to go through and actually read in detail and at the end of the day I feel like, it might be a generational thing, but you kind of go into these services knowing that some of your information will get out, and with some services more so than others, you’re more diligent about it….I also don’t know if I would put too much weight on their privacy policy just because, of course, nobody is going to say ‘*We’re going to sell your information to data mining companies*.’ <laughs> It seems like it would be generic language.

Although most participants were inclined to trust Fitbit by default to handle their data appropriately, some were more pragmatic, and called out their uncertainty as a reason to not share overly sensitive information with the company. For example, one person noted that “I actually imagine that [Fitbit doesn’t keep my data secure], and this is another reason why I haven't been totally into uploading blood glucose measurements and stuff like that. They, obviously, have all sorts of data problems. They had a data glitch a while back where they erased two weeks of my data, and, yeah, they're obviously having problems updating their data daily.”

Regardless of whether they do actually trust the company, most individuals based their judgments about trust on their ideas about the company’s business model or their personal experiences with customer service. One user looked to Fitbit’s socially beneficial, health-related mission as a clue about the company’s integrity: “From a logical perspective, I’m impartial, but I’m inclined to trust Fitbit because of…it’s the same reason I think a lot of us are more inclined to trust Whole Foods even though there may be reasons not to—because they kind of have that, ‘*I’m trying to do good, I’m bringing forth something that is natural or to help people*,’ and so you kind of automatically trust them. Certainly their goal is to make money, make a profit, but *the idea of providing a device that’s out there to help you lose weight or just be more healthy, you would think that they have some positive goals in mind*.”

The most common solution to the problem of insufficient information about Fitbit’s trustworthiness was to outsource fact finding to others: “Typically I trust other people on the Internet [to flag problems for me]… I keep up with…what's going on in Reddit and Hacker News and all this stuff and so I feel like if somebody was doing something [wrong] with customer data…I would have…or will see [that information] somewhere." Another participant said, "I always figure that if something really stinks, people will kick up a fuss…I always hope that someone who is really invested in that kind of stuff will kick up a stink if there's something really untoward going on but I'm personally too lazy. And it's always sort of clouded with lawyerese and it's unfathomable what exactly they mean. *And besides, I would just say 'yes' anyway because I want the service, so I wouldn't turn it down*."

(5) Suggestions regarding building trust:

- Explain to users what steps the company takes to establish privacy-protective procedures, including:
    - Whether the company has a Chief Privacy Officer or other privacy staff;
    - How the company has built privacy into their systems, by design;
    - What concrete steps the company has taken to ensure that users' contextual privacy preferences are observed, particularly with regard to information distribution to insurance companies, employers, pharmaceutical companies, law enforcement, or other third parties for whom health information is valuable or may present privacy-related discomfort to users;
    - What privacy and security training their officers and employees have received, and how frequently;
    - Whether the company has received privacy complaints from individuals, the press, the FTC, or other entities, and if so, how those complaints have been resolved.

- Be sensitive to the fact that health self-tracking companies may benefit from a privacy "halo effect" by virtue of their socially beneficial products; this may leave customers especially vulnerable to not doing due diligence regarding information privacy and security.

- Encourage users to share concerns about privacy and security with the company; maintain a list of those concerns, and take concrete steps to address them. Consider posting these concerns and actions online.

Participants in this study…

(6)…express highly granular health information flow preferences that are tailored to specific business or social contexts. Of all the privacy concerns flagged by the individuals I interviewed, cross-contextual information flows were the most commonly expressed and were the most deeply worrisome. Participants were particularly cautious about their health information being shared with social networks, their employers, insurance companies, and marketers; most also preferred not to share information with law enforcement. Information flow preferences were closely linked to data type, as well. As was discussed above, many of the individuals I spoke with were reluctant to share certain kinds of information (e.g., diary entries, blood pressure, blood glucose levels) with self-tracking services because they were uncertain of how that information would be used and where it might end up.

In a forthcoming report, I detail the granularity of these information-sharing preferences as a function of particular *information type* x *information recipient* combinations.[58] But as a general matter, the people I spoke with prefer to keep their health and wellness information contained within the realm of health and wellness, and particularly to staunch potential data flows to the following entities:

- **Social networks**. Every person I interviewed drew a clear distinction between wellness and fitness social communities and other social media, like Facebook and Twitter; and most were vehemently opposed to sharing health information across services. Although nearly every person had a Facebook account, for

[58]

example, not one preferred to log in to Fitbit via Facebook Connect. Every person I spoke with except one had deliberately opted not to broadcast health data to social networks. Routinely, people said things such as, “There’s some value to separating Facebook from everything else. *I don’t want my [Fitness] stats published on Facebook ever. I have something like 900 friends; it’s become a place to read news and comment, but I’m very wary of putting out personal information.*”

Some of this discomfort originated from fears of embarrassment should health information inadvertently be reposted by family or friends, and make its way to people who would judge them negatively. “I've consciously opted out [of logging into Fitbit with] Google Plus and Facebook, I always worry that somehow it's going to pop up on my Facebook feed and suddenly start logging my weight or something.” Another woman envisioned possible social stigma: “Let’s say it’s a young--well, I guess any person, but I would use a young person for this example--information gets out that they have some sort of STD or STI, or something like that, and people can be really cruel, and if people--everyone else finds out, they can judge you or look at you sidewise and stuff like that, and in that case, you don’t want that getting out.”

Most people were also mindful of norms around sharing information, even with friends, and particularly where information is contextually inappropriate for a given environment: “I also don’t want to spam my friends. I feel sending out my steps is spamming in a lot of ways. And I do it anyway because it’s a motivator for me…. [But] so, things like weight, blood pressure, blood sugars, these are things that probably-- that would be really spammy to send out to my friends.” Another woman explained that she’s mindful of sharing too much with other social network *companies*: “My Facebook friends don’t necessarily need to know that I’m doing all of this [Fitness tracking]. They can and I’m not trying to keep it a secret, but it doesn’t need to be shared with the world all of the time, and it’s also just sometimes I worry about exactly how much of my life Facebook knows.”

Like this woman, some other people flagged that large social networks are simply becoming too expansive—they know "too much" about individuals: "I think that Facebook does a lot of damage as it is with knowing too much about people. I'm not a big fan of Facebook anymore. I don't like that my Facebook would have all these things, so most apps that I have on my phone or something they're like, 'Oh, log in with Facebook,' and I try to avoid that, because then I feel like it lets Facebook know too much, and people track too much things on that."

Most users also explained that they prefer social network services to occupy separate functional spheres. As a general rule of thumb, people I interviewed used Facebook for communicating casually with family and friends, Twitter for sharing and receiving information about work, Fitbit for sharing information about light-natured health and wellness issues, and health support groups for discussing more specific and intimate health issues. To cross these boundaries would not only cause embarrassment or disrupt expectations about the types and amounts of information it is appropriate to share online, it would cut against the grain of the user's own expectations about purpose of the service itself. Said one woman who works in library science and uses Twitter mainly for work, "'I walked 10,000 steps today,' or 'I ate this today,' is really not in the vein of what my Twitter is trying to achieve. It's not books, it's not publishing, it's not libraries. It's not talking to or about authors. I mean, I also go back and forth with my friends about stuff. I mean, I tweet about random stuff also, *but [health and wellness is] just a little too far removed from what my Twitter is supposed to be about*."

A young woman who copes with a chronic illness explains how fitness tracking differs from other kinds of health tracking: "In my life, [health and wellness] are the same, they go hand in hand, but really they're very different. There's even—like, I message people on Fitbit and there's a guy who is…way up, he's like, number three on my list and…we chat back and forth. And he was offering encouragement. And I had been [sick] recently and one of the things he said is, ‘Hey, I’d really like to see your stats go up,’ and try and offer encouragement. He doesn’t know that I’ve been [sick] and my stats dipped because I was lying curled up in bed all weekend. And I could tell him, but he doesn’t really need to know that part of my life.”

To shore up these contextual boundaries within the social realm, some users register with services using different email accounts. One person I spoke with, for example, has an email account for communicating with trusted or valued services, such as his Internet Service Provider, his electric company, and LinkedIn (his “professional identity online”), and a separate email account for “junk” social sites. He elected to register Fitbit with his primary email account as an expression of its elevated status relative to other social services: “I have two emails. I have this one on Gmail and I have like kind of a social media ‘junk’ kind of Gmail that I would’ve normally put for something like [Fitbit], but I feel like *since I take this Fitbit thing a little more seriously*, I use this [real one]….But, the other email that I use is like for LivingSocial and Groupon stuff.”

- **Employers**. Top of mind for many participants were potential employment and insurability harms associated with an unexpected flow of quasi-medical data, even if they were not personally grappling with a health issue. Participants generally felt that extra information in the system would be more likely to cause harm than to help one’s career. Although people I spoke with enjoy their jobs and have positive relationships with their supervisors and colleagues, most also expressed the sentiment that they’re at work to perform a function, and “they don’t need to know [too much] about what I do when I leave.”

  Participants were particularly mindful of accidentally divulging information that would promote a sense of instability or untrustworthiness, or that would run the risk of raising an employer’s insurance rates. A man explaining why he would not want information about his mental states to be revealed to his employers said, “I think depending on what your moods are, you could--maybe you’re viewed as unstable. And I don't need [my employer] thinking that I'm unstable, and I don't need them thinking anybody else is either." A man who manages diabetes echoed these concerns, which for him are not hypothetical, "I don't want an employer or a potential employer to go and find all my diabetes, all my blood pressure, blood glucose, and weight, and all this other medical information, and then say 'This guy's going to drive our healthcare [costs] up.' And so, I don't even get the interview because [a potential employer] has just tremendous insight into my health before he even contacts me."

A man flagged the possibility that, "so if my boss had a Fitbit and they were [on the service] and I was like, 'Oh, I was home sick all day,' and they looked, and it's like, 'Well, you have really high activity levels-- What were you really doing?'. So, I think [health monitoring data] could be used against you like that. Yeah, those kinds of things for monitoring unnecessarily."

And at bottom, many people simply felt that to narrow the separation between social life and work is not necessary: "it's irrelevant [for my employer] to know if I exercise or not unless it has a conflict with my job, and it doesn't. I'm not running into burning buildings [for a living]."

- **Insurance Companies**. Nearly every person I spoke with regarded insurance companies with mistrust and fear, frequently referring to raised rates and the inability to qualify for coverage. Some expressed feeling similarly trapped by insurance companies in real life: two participants had been denied health insurance coverage in the past due to diagnostic codes in their medical records; one without benefits for two years. Another is currently afraid to change jobs because she is concerned that a diagnostic code in her records will prevent her from being covered again. One is concerned about whether her chronic illness will make her ineligible for health insurance when she leaves her parents' plan.

Typically, people I spoke with only felt comfortable with insurance companies having the information strictly necessary to reconcile medical claims. This included the administrative categories of age and location, as well as specific health data such as current medications and recent lab test results. The most common refrain, by far, was some variant of “I don’t WANT insurance companies to have my information, but they’re going to get it anyway.”

Even when insurance companies are educating participants about their health conditions, participants feel more threatened than appreciative: “So my insurance company knows all of the medications that I'm on. They have correctly inferred a couple of my health problems, and have been sending me literature about such. So they're like, ‘Oh, you're on Metformin and Levothyroxine. You have thyroid and diabetes problems, and so here's some booklets, and here's help desk nurse that you can call any time if you have any type of problems’…. I mean, I'm not going to call my insurance company's help desk nurse because I don't trust them. *They're incentivized to screw me over, and so I do not like that*.”

Three other people flagged that if health tracking information reached insurance companies, they or family members could face difficulties: One woman explained, that, “Two years ago I was almost killed in a bike accident and…I was life-flighted off a mountain and lucky to survive and I still ride because it means a lot to me. So if they still knew I ride-- …if they still knew how often I ride…they probably wouldn’t be very happy about it because it could happen again.” Another woman relayed a story about her mother controlling a medical condition with an off-label use of a drug: “For example, I know that my mom was on some medication that’s for narcolepsy. My mother does not have narcolepsy, and at some point the insurance company was like, ‘No, we’re not paying for this drug anymore because she does not have narcolepsy.’ So…at some point my insurance company figured out that my mother does not have narcolepsy.” A man who is active in martial arts said, “I would let [insurance companies] know [about my physical activities] if it’s relevant to a claim or something like that. But otherwise probably not…I say that because I was in a car accident a bunch of years ago and they asked that question to see if my injuries were due to Jujitsu, or working out, or the accident. I was, 'Hmmm."

- **Commercial Researchers**. When discussing commercial researchers and marketers gaining access to their health and wellness information, the people I spoke with slipped readily into a harms discourse. Even where the nature of this work (e.g., research) was itself viewed positively, commercial researchers were not granted the assumption of benevolence. One participant called commercial researchers, "greedy and horrible"; another doubted their commitment to helping society: "I guess I just don't trust that [commercial researchers are] actually-- I think it can be really invasive and-- yeah. I mean, I think I just feel like very few people are benefiting from [pharmaceutical research], and it's no longer about helping people but [is] about easiest medication, fastest medication, most money, most cost-effective. So I think that's why I have an aversion to it." Another does not want commercial researchers to have access to her health information because, "It's all about, you know, lobbyist and money and it's not based on [facts], and I'm not so interested in those skewed results, I guess. I mean, like, university research can be skewed, too, but it's more neutral, I think." To the extend that people were willing to share their health information with commercial researchers, it was on the condition that the data be de-identified and aggregated, and only for a particular cause that the user cared about.

- **Advertisers**. As with commercial researchers, participants in this study took a dim view of their health information being shared with advertisers or marketers. Some were cautious about exploitation: "Advertisers and marketers will just exploit my information to sell me things. In theory it's ok with me that marketing exists, but I [still] prefer that they not know [things about me]." Others were dubious about marketers keeping their information secure and using it for socially beneficial purposes: "I'm not willing to give [advertisers]…information because I also don't feel that they have any incentive to keep that information private or to use that information for good." One person said she would not mind receiving personalized advertisements for products that were relevant to information she makes public, but that she would be uncomfortable if her data flowed beyond a privacy wall that she erected by virtue of managing her privacy settings: "For instance, if I had high blood pressure, and I put [that] in [Fitbit] but it was private [in the privacy settings], and I started getting medical [ads] for blood pressure [products], I would be really weirded out. That would be scary, right?"

(6) Suggestions regarding contextual information flow preferences:

- Consider that users want granular privacy control over all types of health information in their possession.

- Respect that although individuals may be comfortable sharing some kinds of health information with other fitness or food consumption tracking services, they may want to establish firm boundaries between other, seemingly-related services, such as:
  - Social networks without a health or fitness aspect;
  - Health networks that are specifically clinically/medically oriented;
  - Insurers, even where rate reductions are possible;
  - Employers, even for purposes of employee wellness programs;
  - Commercial health research, except where data is anonymized and specific research programs are approved individually; and
  - Behavioral marketers

- Where any information disclosures to the above entities occur, inform users of this disclosure, and explain exactly what information is being transmitted, to whom, for what purpose, for how long, and what steps users can take to reduce or stop that disclosure.

Participants in this study…

(7)…take an expansive view of health privacy harms. Although users flagged concerns about stalking and other criminal activities, as well as worries about behavioral advertising, employment discrimination, or insurance pricing, other risks were wide ranging and varied in their severity. Many users I spoke with were sensitive to unexpected attributes of tools or their use. Even simple and seemingly ill-considered design choices can cause embarrassment—such as pictures of toilets or a stomach to depict apps for gastrointestinal illness, icon designs that caused a woman I interviewed, a sufferer of ulcerative colitis, to be fearful of letting others use her phone lest they see these images on her home screen. In fact, several users noted that they use health self tracking services to record or share only the health information they are proud of already—or at least not embarrassed about. A woman explains that she shares her fitness counts but not her weight with other Fitbit users because, “I’m proud of my steps [count]. I’m not proud of my weight.” Other users described even ordinary Fitbit usage with embarrassment, chastising themselves for appearing “obsessive compulsive,” and fearing being tagged as a Fitbit user to their friends in real life. Many times, these individuals not want to be perceived as “self-involved,” “narcissistic,” or simply “the kind of person who tracks.” One woman says, “I tend to not tell everybody how much I track because as soon as I do I get the funny look and I get all defensive and stuff.”

(7) Suggestions regarding unanticipated user sensitivities:

- Appreciate that health self-tracking may be particularly stigmatized for users, and that they may want to be discrete about the mere act of tracking certain metrics.

- Be aware that users may present with unanticipated privacy sensitivities, and build flexibility into the system to help accommodate these preferences. For example, allow users the option of less graphic icons on their smart phone desktops, or provide users with a ‘Quick Exit page on the website portal.

Participants in this study…

(8)…want the ability to view, correct, and download their own data.

(8) Suggestions regarding user access and corrections:

- Anticipate that users may have many reasons for wanting accurate and complete health data:
    - To manage a particular health condition, such as weight or blood pressure;
    - To improve health metrics, such as sleep quality or running distance;
    - To reduce undesired behaviors, such as over-eating or smoking;
    - To find specific correlations between different behaviors or health biomarkers, such as alcohol consumption and mood;
    - To provide care for someone else;
    - And more.
- Anticipate that users may want to share select portions of their accurate health records with family and friends, coaches, medical doctors, or other trusted health guides.
- Explain to users what steps the company takes to establish procedures for ensuring data accuracy, such as:
    - Employing data scientists, health specialists, or other personnel who can evaluate the quality and integrity of the health data; or
    - Using sensors that fall within particular accuracy tolerances.
- Teach users how they can improve sensor accuracy and reliability, such as recalibrating a smart weight scale, or wearing pedometers on a particular region of the body, such as the waist, or orienting the device properly, or controlling temperature or walking speed.
- Explain to users whether, under what circumstances, and how they can correct, augment, or delete their own health data.
- Explain whether the company has received data accuracy or reliability complaints from individuals, the press, the FDA, or other entities, and if so, how those complaints have been resolved.

Participants in this study…

(9)…feel vulnerable in an unregulated environment. Many people I spoke with refrained from divulging detailed health information with health self-tracking services because they believe this area to be under-regulated. About half were mindful that very few legal protections inhere in health information stored by Fitbit or other commercial entities. This knowledge influenced their decision to not record health data on the Fitbit website: One user explained that he would not use Fitbit to log is blood glucose levels because, "A doctor can't tell anybody [that] I have diabetes, it's HIPAA prohibited, so--but here, [Fitbit], you know, isn't subject to HIPAA regulations or anything, anybody can look at it. Fitbit is not a medical organization, it's not bound by the rules of a medical organization, so I wouldn't want them, you know, [to have my blood glucose levels]. I would have no recourse [in case of unwanted information flows]."

In contrast, a woman explained that she was willing to share information with her doctor because, "I assume that what goes on between a doctor and patient is fairly well protected, just by government laws, I mean almost the fundamental human right to have some facts about you not be shared. It's not part of the Hippocratic Oath but it feels like it's almost as fundamental as that because a lot of it can be used against you. I mean unless you pose immediate public health risk, I think most data I hope would be protected by some kind of privacy law unless you dispense-- you give the doctor permission."

Another person complaining of behavioral advertising noted ruefully that, "there are privacy laws and there are spam laws and whatnot but there's nothing really...if Fitbit sold my information to an advertiser and they sold let's say my weight, there's nothing saying that an advertiser can't then just create an ad that says, 'John's weight is X.' You know? And I wouldn't put it past them."

(9) Suggestions regarding communicating legal restrictions:

- Tell users which privacy laws or principles (such as the FIPPS) govern or guide the company's data management practices.
- Provide links to applicable laws and explain, briefly and clearly, and with examples, what steps the company takes to ensure compliance, and what recourse individuals may have should they have a grievance.

V. Summary

Participants in this study engage deeply with commercial health and wellness tools. They enjoy the benefits of tracking and sharing—greater health awareness and a sense of control and accomplishment—but they also care about the privacy of their health information flows, and they struggle to operationalize those preferences. Not only do they give up a vast quantity of highly detailed behavioral information by wearing self-trackers almost continuously, they underestimate the quantity and detail of demographic and anatomical data that they have linked to their accounts. Being complete and truthful allows them to take full advantage of their purchase and receive accurate health feedback. This is compelling logic. But when compelling logic meets significant challenges—to understanding and customizing privacy settings; to comprehending back-end information flows; to making rationale judgments about the security of a company's data management practices—these users are putting themselves at risk. Ironically, their sensitivity to potential harms, particularly around violating social norms or risking their employability or insurability, appears to result in a deliberate withholding of some kinds of information that would lead them into troubling situations for which there is currently no legal recourse. The people I spoke with are largely aware that commercial health and wellness services are operating in a relatively unregulated environment, and are respond to this with a combination of resignation, cynicism, and fear. The dominant reaction is simply to opt out—to take self-protective measures to shield themselves from future harm, thus leaving them less able to experiment with and enjoy innovative new technologies on the horizon.