VIRGINIA JOURNAL OF LAW & TECHNOLOGY

WINTER 2015 UNIVERSITY OF VIRGINIA VOL. 19, NO. 02

An Emergency Room in Your Living Room: Privacy Concerns as Health Information Moves Outside of the Traditional Medical Provider Context

ADAM STEELE†

† Adam Steele is an administrative law attorney with Styers & Kemerait, PLLC, in Raleigh, North Carolina, and received his J.D. from Campbell Law School. He would like to thank Campbell Law School Professor Amy Flanary-Smith for her guidance and support in writing this article and throughout law school, as well as Professors Sarah Ludington and Margaret Currin for their useful feedback and suggestions. Finally, he is grateful for his wife, Shannon, for her support and inspiration regarding the topic of this article.

ABSTRACT

The consumer health monitoring industry is expanding at a rapid pace as lifestyle tracking device makers like Fitbit and smartphone manufacturers like Apple introduce consumers to the idea of tracking every workout. Devices that track and analyze more sophisticated health information are entering the consumer market as well. This article examines the consumer health device industry and the underlying privacy risks faced by consumers when using these devices. The Article discusses the current state of federal regulation of consumer health devices, examines the need for privacy regulations, and concludes with a proposal that the Federal Trade Commission take a two-pronged approach to protect consumer privacy interests.

TABLE OF CONTENTS

I. Introduction 393

II. Background on consumer health devices 400

A. Current fitness trackers collect and monitor CGLI 401

B. Smart devices and the accompanying accessories currently monitor CGLI but are beginning to include features to track CGHI 402

C. In-home consumer health devices are introducing consumers to CGHI monitoring 404

III. Current protection of consumer-generated lifestyle and health information 406

A. Device makers self-regulate the handling of CGLI and CGHI through terms of service and privacy policies .. 407

B. FDA authority over consumer health devices is limited to safety and effectiveness regulations rather than privacy 411

C. HIPAA is applicable only to covered entities collecting protected health information 416

D. The FTC has the authority to protect and define consumer privacy expectations 418

IV. Regulation of consumer health device makers should be pursued while balancing the need for innovation with the strictures of regulatory compliance 422

A. Past consumer data breaches show the need for protection of CGLI and CGHI, despite the potential regulatory costs to the consumer health device industry 424

B. Maintaining the status quo by leaving consumer protection to the market is an insufficient solution 429

C. Expanding HIPAA's definition of covered entities to include consumer health device makers would prove too unwieldy a solution 437

D. The FTC, to protect consumer privacy interests, should utilize its current enforcement authority to protect CGLI in the short term and develop needed rules governing CGHI protection in the long term 441

1. Enforcement actions under the FTC Act should be utilized in the short-term to protect consumer privacy expectations in CGLI 443

2. Targeted rulemaking to proactively address privacy concerns in the CGHI-monitoring industry should be developed and adopted 447

V. Conclusion 453

I. INTRODUCTION

In July of 2011, a number of Fitbit users had an embarrassing aspect of their personal fitness data put on full display for the world. While many exercise enthusiasts would gladly welcome the ability to boast about their latest running, swimming, or biking achievement, these users had a more personal activity conveyed to the world: their sexual activity.[1] A simple Google search turned up voluminous results showing when the users' sexual activity began, how long the activity lasted, and a sometimes very detailed description of the sexual activity.[2]

The issue was not that Fitbit, a supercharged pedometer that is primarily used to track fitness activities—e.g., sleeping patterns—and the resulting calories burned,[3] was recording sexual activity; users, after all, were choosing to record the activity themselves. Rather, the issue was that the default sharing setting for the device and Fitbit tracking service was set to "public," leading many of these users to fail to realize their sexual activity statistics were in public view until seeing the headlines on the internet.[4] Fitbit quickly moved to set the default sharing setting to "private," hid users' activity-tracking

---

[1] Kashmir Hill, Fitbit Moves Quickly After Users' Sex Stats Exposed, Forbes (July 5, 2011, 7:58 AM), http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed.

[2] Chris Matyszczyk, *TMI? Some Fitbit users' sex stats on Google search*, CNET (Sept. 9, 2014, 11:03 AM), http://www.cnet.com/news/tmi-some-fitbit-users-sex-stats-on-google-search.

[3] Nathan Chandler, *How FitBit Works*, HOWSTUFFWORKS, http://electronics.howstuffworks.com/gadgets/other-gadgets/fitbit.htm (last visited Mar. 2, 2014).

[4] Hill, *supra* note 1.

details on its website, and contacted various search engines to have the data scrubbed from search results.[5]

This simple example highlights the hazard a consumer may face when taking advantage of the latest and greatest consumer device to monitor his lifestyle and health information: exposure of that sensitive information beyond the confines of the monitoring device or service. The "gamification" of health care[6] has caused an incredible surge in consumers monitoring their own lifestyles or health information, whether through gym programs, information tracking devices, or social networks. The consumer health monitoring industry, however, is not one-size-fits-all; while fitness trackers currently receive the greatest amount of attention from consumers and retailers, more sophisticated devices are soon likely to be exploding in popularity as they hit the consumer market as well.[7]

---

[5] *Id.*

[6] *From Fitbit to Fitocracy: The Rise of Health Care Gamification*, KNOWLEDGE @ WHARTON (Jan. 16, 2013), http://knowledge.wharton.upenn.edu/article/from-fitbit-to-fitocracy-the-rise-of-health-care-gamification/ ("[These games] invented by health insurers and a host of technology startups, are marketed directly to consumers, who use them to track their progress and record key health metrics such as blood sugar and pounds shed. Players of these games can win rewards, perhaps even cash, if they hit their health goals."). For a discussion on increasingly incentivized personal data tracking—including tracking of health data—and the resulting privacy implications, see Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of A Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1169 (2011) ("[It is] easy to imagine why individuals or employees would use remote health monitoring systems to secure discounts. A health-conscious employee who carefully controls her diet and exercises regularly may see such discounts as a justified reward for healthy behavior.").

[7] *CEA Releases Report on Dramatic Rise of Connected Health and Wellness Consumer Devices Market*, BUSINESSWIRE (Jan. 2, 2014, 3:49 PM),

The consumer-generated information specifically at issue can be divided into two distinct groups: lifestyle information and health information. Consumer-Generated Lifestyle Information ("CGLI") consists of information based upon activities that a user engages in throughout the day, such as exercise, sleeping, and eating habits. CGLI is currently collected and monitored primarily by fitness trackers, like Fitbit devices, but is increasingly being monitored by smart devices, like smartphones and smartwatches. Fitness trackers and smart devices alike can be used to monitor CGLI automatically, like exercise and sleeping habits, or monitor CGLI manually, like eating habits.[8] The CGLI is then synced, most commonly, with the device maker's fitness or health-related service.[9] The information based upon the consumer's physical condition while wearing the device can then be used to provide instant feedback or long-term monitoring of the consumer's physical well being.

---

http://www.businesswire.com/news/home/20140102005942/en/CEA-Releases-Report-Dramatic-Rise-Connected-Health ("[T]he analysis forecasts that the evolution of U.S. healthcare will result in a more than 142 percent increase over the next five years in personal health and wellness product sales and software and service revenues.").

[8] For example, Fitbit uses a pedometer within its devices to monitor automatically steps taken while also allowing users to link manually-entered daily nutrition information to the Fitbit user's Fitbit.com profile. This information is manually entered into other services that then transmit the information to Fitbit via the Fitbit API ("application programming interface"). *See How do I get data from my tracker to the website?*, FITBIT, https://help.fitbit.com/customer/portal/articles/896922-how-do-i-get-data-from-my-tracker-to-the-website (last visited Apr. 7, 2014).

[9] There are multiple ways for devices to sync collected health information. For example, Fitbit devices typically sync with a computer via a USB wireless dongle or smartphone via Bluetooth, and then that information is synced with the user's Fitbit.com account. *Id.*

Consumer-Generated Health Information ("CGHI") consists of information customarily considered to be "Health Information" collected by a traditional medical provider, like a health care professional.[10] This information can include, for example, a user's temperature, heart rate, blood pressure, electrocardiography, and heart rate variability.[11] Rather than visiting a doctor's office, a consumer can remain at home while he automatically monitors, collects, and analyzes his health information through CGHI-monitoring devices.

At present, CGHI-monitoring devices are much more accurate and sophisticated, albeit less prevalent, when compared to CGLI-monitoring devices. CGLI-monitoring devices, however, are introducing and popularizing the idea of monitoring "health"-related information. As the technology behind these devices naturally and quickly progresses, the distinction between CGLI and CGHI-monitoring devices will be blurred; devices monitoring consumer-generated *lifestyle* information will continue to advance to the point where the devices are capable of monitoring consumer-generated *health* information as well. In fact, some devices which would be

[10] For a point of reference, health information is defined under HIPAA as "any information, whether oral or recorded in any form or medium, that . . . [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103 (2014). However, for health information to be under the purview of HIPAA it must also be "created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse." *Id.*

[11] *infra* note 41.

more likely to be classified as CGLI-monitoring devices are already capable of monitoring a user's heart rate.[12]

A consumer could certainly benefit from the ability to know more about his lifestyle and health as these devices flood the market, but that same consumer will also face a number of privacy concerns regarding how device makers collect, maintain, and use his CGLI and CGHI. While CGLI and CGHI offer two shades of sensitive health-related information, the Fitbit example discussed at the outset demonstrates that a breach of a consumer's CGLI—information that is increasingly becoming more accurate—could prove just as damaging as a breach of his CGHI or other private information.[13] Moreover, breaches of consumer privacy expectations can occur in a variety of manners, and a device maker could increase the risk of unintentionally breaching its users' lifestyle and health information by aggregating and exploiting that information to

---

[12] For example, the newly-announced Apple Watch is described as "a 'comprehensive' health and fitness device" that features a sensor to continually track a user's pulse rate. Ben Fox Rubin, *Apple jumps into wearable fray with Apple Watch smartwatch*, CNET (Sept. 9, 2014, 11:03 AM), http://www.cnet.com/news/apple-dials-up-apple-watch-smartwatch/; *see also infra* Part I.b and note 32.

[13] *See* David Ranii, *Raleigh-based Valencell's technology powers new wave of wearable fitness products*, NEWS & OBSERVER (Feb. 22, 2014), http://www.newsobserver.com/2014/02/22/3643723/raleigh-based-valencells-technology.html ("Valencell's technology is a step forward from the current crop of fitness-oriented wearable devices, which are dominated by what are essentially high-tech pedometers or require the user to wear a chest strap. . . . Valencell's technology operates by shining an LED light on your skin—in your ear, for example, or on your arm. A tiny portion of that light actually penetrates your skin and bounces off your blood vessels, creating a waveform that is detected by an optical sensor to measure your blood flow with each heartbeat. That leads to readings on key metrics such as heart rate, calories burned, respiratory rate, blood oxygen level and aerobic fitness, or VO2 max.").

increase profits.[14] Other concerns can include intentional breaches from malicious attempts to access the information by outside entities or individuals,[15] a failure by the device maker to maintain the information properly,[16] or even inadvertent breaches by the consumer himself.[17]

---

[14] *See* Matt Marshall, *How Jawbone is using big data to lead the personal fitness-wearable industry*, VENTUREBEAT (Nov. 6, 2013, 8:45 AM), http://venturebeat.com/2013/11/06/how-jawbone-is-using-big-data-to-lead-the-personal-fitness-wearable-industry ("Jawbone gets its data through a clever exchange. First, it offers an easy-to-use way to monitor your activity, in exchange for the access to your data. It has since gathered such massive amounts of data that it can uncover patterns that would be missed by experiments of smaller scales. The company feeds personalized advice back to each of its customers, increasing the value of its basic service, but also enabling it to tailor its updates to products and services to a user base it knows more intimately than ever."); *see also* Dana Liebelson, *Are Fitbit, Nike, and Garmin Planning to Sell Your Personal Fitness Data?*, MOTHER JONES (Jan. 31 2014, 6:00 AM), http://www.motherjones.com/politics/2014/01/are-fitbit-nike-and-garmin-selling-your-personal-fitness-data.

[15] *See, e.g.*, Ben Kuchera, *PlayStation Network hacked, data stolen: how badly is Sony hurt?*, ARS TECHNICA (Apr. 26, 2011, 7:37 PM), http://arstechnica.com/gaming/2011/04/sonys-black-eye-is-a-pr-problem-not-a-legal-one (discussing the 2011 hacking of Sony's PlayStation Network and the company's decision to wait almost a week before informing customers of the data breach).

[16] *See* Ben Kuchera, *Sony admits utter PSN failure: your personal data has been stolen*, ARS TECHNICA (Apr. 26, 2011, 4:24 PM), http://arstechnica.com/gaming/2011/04/sony-admits-utter-psn-failure-your-personal-data-has-been-stolen; *see also* Rich McCormick, *Weak hospital security means hackers could steal medical records and ruin blood supplies*, THE VERGE (Apr. 28, 2014, 6:06 AM), http://www.theverge.com/2014/4/28/5660564/poor-hospital-security-at-risk-from-hackers.

[17] *See* Wesley Fenlon, *5 Ways to Keep Your Information Secure in the Cloud*, HOWSTUFFWORKS, http://computer.howstuffworks.com/cloud-computing/5-ways-to-keep-your-information-secure-in-the-cloud.htm (last visited Mar. 3, 2014) ("Web site security often allows hackers easy access to boatloads of personal information. We can blame corporations for poor

Regulations from agencies that already oversee, or are likely to oversee, these device makers, such as the Food and Drug Administration ("FDA") and the Department of Health and Human Services ("HHS"), are not currently applicable or sufficient to protect consumers from breaches of this private information and the subsequent abuses that can occur. Often the only recourse consumers have is from the specific device maker's terms of service or privacy policy; however, changes to existing regulations and enforcement actions could provide the protection that consumers expect when using these collective "Consumer Health Devices."

Recognizing a need for greater consumer protection in the CGLI and CGHI-monitoring industry, the Federal Trade Commission ("FTC") announced in December 2013 that one of its primary areas of focus in 2014 would be the increasingly widespread use and accompanying privacy implications of consumer-generated health information.[18] The FTC held a public seminar in May of 2014 to address a number of issues surrounding consumer health devices and the associated CGLI and CGHI.[19] FTC officials answered questions from the public and discussed issues that included identifying what products and services consumers are using to generate and control their own health data; determining who is behind the products and services; and examining what actions are being taken by these

---

security and hackers for maliciously attacking Web sites, but there's a third party often at fault in these attacks: ourselves, the users.").

[18] *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues*, FTC (Dec. 2, 2013), http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues .

[19] *Spring Privacy Series: Consumer Generated and Controlled Health Data,* FTC, http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data (last visited Aug. 14, 2014).

device makers and service providers to protect consumers' privacy and security. The FTC also sought to determine the level of consumer expectations regarding privacy and security protections from these companies, particularly to determine if consumers view these devices and companies differently from traditional medical products and entities already covered by the Health Insurance Portability and Accountability Act ("HIPAA").

Part I of this article will examine the current state of the consumer health device industry, specifically focusing on devices that monitor CGLI or CGHI. Part II will then discuss the privacy policies of various industry-leading consumer health device makers, as well as the current state of FDA, HHS, and FTC regulation of consumer health devices. Finally, Part III examines the need for privacy regulations and proposes different means of regulation to protect consumer privacy interests.

II. BACKGROUND ON CONSUMER HEALTH DEVICES

Fitness trackers, smart devices and applications, and in-home monitoring devices are just small pieces of a growing industry in today's data-driven society. Fitness trackers allow users to track lifestyle habits both automatically and manually.[20] Smartphone manufacturers are beginning to ship smartphones and smartwatches with heart rate monitors and other health-monitoring features, as well as platform-specific applications that aggregate users' lifestyle information to provide "fitness coaching" and instant health analysis.[21] In-

[20] *See infra* Part I.a.
[21] *See infra* Part I.b.

home monitoring devices allow consumers to collect and identify even greater detail about household members' health, possibly even saving a trip to the doctor's office.[22] Together, these "Consumer Health Device Makers" range from small startups to technology industry giants.

A. Current fitness trackers collect and monitor CGLI

Fitness trackers allow users to track exercise activities, sleep habits, calories burned, and heart rate, among other things. Fitbit[23] and Jawbone[24] manufacture some of the most popular devices in the consumer market. Fitbit provides consumers with a range of devices including a "smartscale," a small pedometer-like device, and more sophisticated wristbands.[25] Jawbone offers a single wristband for fitness monitoring.[26] Each of these devices features comparable fitness tracking ability—namely the tracking of activities, calories burned, and sleep habits—by way of first-party (the device maker's website or smartphone "app") and third-party (other websites or "apps") services. Notably, these devices include manual and automatic lifestyle activity monitoring.

---

[22] *See infra* Part I.c.

[23] *See* FITBIT, http://www.fitbit.com (last visited Mar. 2, 2014).

[24] *See* JAWBONE, https://jawbone.com/up (last visited Mar. 2, 2014).

[25] The Fitbit Aria Wi-Fi Smart Scale "measures weight, BMI and % body fat." The Fitbit Zip "Tracks steps, distance and calories burned." The Fitbit Flex "Tracks steps, distance, calories burned and active minutes [and] Monitors your sleep and wakes you with a silent alarm." FITBIT, https://www.fitbit.com/store (last visited Mar. 2, 2014).

[26] Jawbone's UP allows users to log workouts of all kinds, track calories burned, and the intensity of the workout, as well as "intelligently track" hours slept, light vs. deep sleep and waking moments. JAWBONE, https://jawbone.com/up (last visited Mar. 2, 2014).

B. Smart devices and the accompanying accessories currently monitor CGLI but are beginning to include features to track CGHI

Not content to sit idly by as startups like Fitbit claim their stake in the fitness tracking industry, tech giants like Sony,[27] Samsung,[28] and Apple[29] have also developed devices offering similar or slightly more sophisticated monitoring of consumer lifestyle and health information. Sony aims to incorporate CGLI as only a subset of a smartphone user's data, creating an all-inclusive personal data "Lifelog."[30] Samsung's "smartwatch" devices include features considered standard in a fitness tracker while also including a heart rate monitor, real time fitness coaching, and instant analysis of fitness data in the S Health smartphone app.[31] In addition, Apple has made a strong push into health and fitness tracking through a number of devices and applications. In the recent months, the company

---

[27] SONY, http://www.sonymobile.com/global-en/products/smartwear/smartband-swr10 (last visited Mar. 2, 2014).

[28] Jon Brodkin, *Samsung unveils Gear Fit, a curved, fitness-oriented wristband*, ARS TECHNICA (Feb. 24, 2014, 2:32 PM), http://arstechnica.com/gadgets/2014/02/samsung-unveils-gear-fit-a-curved-fitness-oriented-wristband; Josh Lowensohn, *Samsung's Simband hardware and healthcare platform aim to track your every move*, THE VERGE (May 28, 2014, 2:03 PM), http://www.theverge.com/2014/5/28/5758086/samsungs-simband-hardware-and-healthcare-platform-aim-to-track-your.

[29] Jacob Kastrenakes, *Apple patents headphones that can track fitness and health data*, THE VERGE (Feb. 18, 2014, 10:29 AM), http://www.theverge.com/2014/2/18/5422066/apple-fitness-health-tracking-headphone-patent.

[30] SONY, http://www.sonymobile.com/global-en/products/smartwear/smartband-swr10 (last visited Mar. 2, 2014).

[31] *Samsung unveils Galaxy S5 and new Gear range*, SAMSUNG (Feb. 24, 2014), http://www.samsung.com/uk/discover/mobile/samsung-unveils-galaxy-s5-and-new-gear-range/.

was granted a patent for headphones that monitor a user's "temperature, perspiration and heart rate data,"[32] announced a "HealthKit" application for its mobile operating system, iOS, that will provide "an easy-to-access dashboard where you can monitor important health metrics on a daily basis, while also stepping back to examine your fitness trends over a longer period of time,"[33] and debuted a long-rumored smartwatch that includes a sensor to track, among other things, the user's heart rate and easily share that information with friends.[34]

Smartphones can provide an even lower barrier to entry for a consumer to monitor his own CGLI and CGHI simply because a majority of Americans already own a smartphone, a percentage of ownership that continues to increase.[35] While many consumer health devices are designed to work with a smartphone, technology like that found in the recently released iPhone 6 or Samsung Galaxy S5 can provide similar

---

[32] Mikey Campbell, *Apple patents sensor-packed health monitoring headphones with 'head gesture' control*, APPLE INSIDER (Feb. 18, 2014, 2:09 AM), http://appleinsider.com/articles/14/02/18/apple-patents-sensor-packed-health-monitoring-headphones-with-head-gesture-control.

[33] Chris Welch, *Apple HealthKit announced: a hub for all your iOS fitness tracking needs*, THE VERGE (June 2, 2014, 2:10 PM), http://www.theverge.com/2014/6/2/5772074/apple-healthkit-ios-8-announcement ("HealthKit allows health and fitness apps to share data . . . [and] will also partner with the Mayo Clinic and other health institutions, allowing healthcare providers to receive and transmit data from your checkups.").

[34] Ben Fox Rubin, *Apple jumps into wearable fray with Apple Watch smartwatch*, CNET (Sept. 9, 2014, 11:03 AM), http://www.cnet.com/news/apple-dials-up-apple-watch-smartwatch.

[35] Fifty-five percent of American adults own a smartphone, and twenty-nine percent of all cellular phone owners "describe their cell phone as 'something they can't imagine living without.'" *Mobile Technology Fact Sheet*, PEW RESEARCH INTERNET PROJECT, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet (last visited Feb. 28, 2014).

functionality and remove the need for an additional device.[36] Smartphones also benefit from third-party applications ("apps") that can extend the functionality of both smartphones and accessories alike.[37]

C. In-home consumer health devices are introducing consumers to CGHI monitoring

While standalone fitness trackers and smart devices offer fairly basic CGLI monitoring at present, more sophisticated and complex CGHI-monitoring devices are entering the consumer market as well. At popular tech conferences, like the International Consumer Electronics Show ("CES"), held annually in Las Vegas, Nevada, a number of devices have been unveiled in recent years that will allow a consumer to measure much more than his number of steps taken, sleep patterns, or calories burned.

Some device makers have taken a multifaceted approach to providing a higher level of consumer health

---

[36] The Apple iPhone 6 includes a state-of-the-art "M8 motion coprocessor" that "efficiently measures your activity from advanced sensors." APPLE, https://www.apple.com/iphone-6/technology (last visited Jan. 11, 2015). The Samsung Galaxy S5 "is the first smart phone with a built-in Heart Rate Sensor" and emphasizes the utility of the S Health app. SAMSUNG, http://www.samsung.com/global/microsite/galaxys5/features.html (last visited Mar. 2, 2014).

[37] For example, MyFitnessPal, a free service which can also sync with a Fitbit account, provides users with the ability to input meals and calculate calorie intake. MYFITNESSPAL, http://www.myfitnesspal.com (last visited Mar. 2, 2014). Azumio, a "leader in biofeedback health apps" that have been downloaded over twenty million times seeks to influence behavior and improve its users' wellness through the use of mobile applications and aggregated personal health data. AZUMIO, http://www.azumio.com/about (last visited Mar. 2, 2014).

monitoring at home; one such example is Archos' Connected Self, which includes an activity tracker, scale, and blood pressure monitor that can monitor and analyze a variety of information, such as an irregular heartbeat.[38] Other device makers have chosen a more targeted path in what precisely is being monitored; one such example being a pair of shorts from Athos that can monitor "all kinds of interesting activity in your body, from muscle exertion and lactic acid levels to heart-rate and oxygenation."[39] Other device makers offer an all-in-one device for monitoring CGHI; one such futuristic device is the Star Trek-inspired Scanadu Scout, which allows a user to assess vital signs instantly and with minimal invasiveness.[40] The device allows "anyone to capture important physiological data" by measuring a user's temperature, blood pressure, heart rate, oximetry, electrocardiogram readings, heart rate variability, and stress within seconds of being touched to a user's temple—instantly displaying and monitoring the results on a smartphone app.[41] Scanadu's promotional materials also tout the advantages of its device: recognizing common conditions by combining results with an internet search,

---

[38] *ARCHOS Unveils Complete Selection of Connected Objects during CES 2014*, ARCHOS (Dec. 30, 2013), http://www.archos.com/corporate/press/press_releases/UK_ARCHOS_-_Connected_Objects_301213.pdf.

[39] Ben Popper, *These high-tech gym shorts recorded my muscles as I dunked* on an NBA All-Star*, THE VERGE (Dec. 16, 2014, 12:30 PM), http://www.theverge.com/2014/12/16/7402095/athos-workout-record-muscles-electromyography-jermaine-oneal.

[40] Ben Popper, *Scanadu Scout, the handheld medical 'tricorder' that measures my hangover*, THE VERGE (Jan. 10, 2014, 4:09 PM), http://www.theverge.com/2014/1/10/5294044/scanadu-scout-the-handheld-medical-tricorder-shows-off-its-sleek-new.

[41] *See* SCANADU, http://www.scanadu.com (last visited Feb. 25, 2015).

reducing unnecessary doctor visits, and providing more information to a doctor when a visit is warranted.[42]

With features like these in an array of devices, consumers will certainly be enticed to join the growing ranks of consumer health device users. When a consumer does purchase such a device, he will likely initially be focused on discovering each and every feature of his new gadget rather than how his CGLI and CGHI is being maintained and protected. How these consumer health devices are regulated, if at all, will play a large part in how a consumer discovers his lifestyle and health information has been breached, how he reacts to that breach, and what recourse, if any, he has against the company he trusted with his lifestyle and health information.

III. CURRENT PROTECTION OF CONSUMER-GENERATED LIFESTYLE AND HEALTH INFORMATION

Lifestyle and health information can be protected in a number of ways, but often that protection depends upon the context of the information collected and the entity performing the collection. At the consumer level, a consumer health device user is often left to protect his CGLI and CGHI through lawsuits based on the relational status defined in the device maker's privacy policy and terms of service.[43] Consumers can also be protected by federal agencies like the FDA, HHS, and FTC through enforcement actions and rulemaking. Approval of a device by the FDA is one of the first steps a consumer health device maker may be required to take before going to

---

[42] *See id.*
[43] *See infra* Part II.a.

market; however, some CGLI-monitoring devices may not qualify as "medical devices" for FDA purposes, and FDA regulations do not traditionally include privacy protections.[44] A consumer may be additionally protected by HHS under HIPAA, but only if the entity collecting or maintaining the consumer's health information is a traditional medical care provider, such as a hospital or health insurer.[45] A traditional medical provider's involvement can transform a consumer's health information into *protected* health information; yet, unless this transmission occurs, CGLI and CGHI-monitoring devices remain outside of HIPAA's purview.[46] Lastly, the FTC, through its leading role in consumer privacy issues, has regulatory authority to guide and enforce consumer privacy expectations, as well as experience in protecting sensitive consumer information, including health information.[47]

A. Device makers self-regulate the handling of CGLI and CGHI through terms of service and privacy policies

Terms of service and privacy policies are not new phenomena for modern consumers and will often form the basis of the relationship—effectively one of contract—between a device user and the consumer health device maker.[48] Such terms often guide a company's data retention and security

---

[44] *See infra* Part II.b.
[45] *See infra* Part II.c.
[46] *See infra* Part II.c.
[47] *See infra* Part II.d.
[48] *See, e.g.*, Jack Blum, *Offer and Acceptance in Cyberspace: Ensuring That Your Client's Website Is Protected by Enforceable Terms of Service*, XLVII-1 MD. B.J., Jan./Feb. 2014, at 18, 20 ("Almost every commercial website has terms of service or usage intended to regulate the relationship between the website's proprietor and the users who visit the site.").

policies, but can also assist a company in avoiding liability resulting from a consumer's use of the company's product.[49] While terms of service may be prevalent in today's online-friendly society, the terms are often hidden, long, difficult to comprehend, and possibly inaccurate.[50] And for good reason—using and selling user data can be a very profitable business.[51]

Disturbingly, especially for consumer health device users, the "traditional notice and choice paradigm becomes even more complicated for devices with a limited or no user interface."[52] Because the terms and conditions are presented to consumers on a device with a miniscule electronic display, or

---

[49] *Id.*

[50] G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 165 (2012), *available at* http://www.mttlr.org/volnineteen/hans.pdf.

[51] *Id.* at 164 ("Exploiting user data is a lucrative and effective method for websites to earn money and avoid charging consumers. User data consists of information that . . . can reveal a great deal about the user herself, from individual preferences to biographical information to browsing history."); *see also* Eleanor Harding, *Personal details in smartphone fitness apps 'sold to other firms': 20 most used products pass information to nearly 70 companies*, DAILY MAIL (Sept. 2, 2013, 7:45 PM), http://www.dailymail.co.uk/news/article-2409486/Personal-details-smartphone-fitness-apps-sold-firms-20-used-products-pass-information-nearly-70-companies.html (noting that if "health and fitness information were to be passed to insurance companies, they could use it to set premium prices," and that one such mobile fitness app already earns half its revenue from insurance company partnerships).

[52] Maureen K. Ohlhausena, FTC, *Promoting an Internet of Inclusion: More Things and More People*, 2014 WL 585463 (F.T.C.) (Jan. 8, 2014). For a report on the "notice and choice paradigm," also see *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress,* FTC, http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission (last visited Mar. 3, 2014).

possibly in a comparably low-tech leaflet included in the box, many users of these devices may not bother to read the terms at all before blindly agreeing, "particularly if [the terms are] written in a very small font and they are viewing it on a cell phone."[53] Despite this fact, these so called "clickwrap" agreements are often held to be enforceable against consumers.[54]

Some of the most popular consumer health device makers have the seemingly standard terms of service that include provisions detailing the use of "user generated content," limitations of liability, and conflict of laws provisions.[55] In addition, device makers often include privacy

---

[53] *From Fitbit to Fitocracy: The Rise of Health Care Gamification*, KNOWLEDGE @ WHARTON (Jan. 16, 2013), http://knowledge.wharton.upenn.edu/article/from-fitbit-to-fitocracy-the-rise-of-health-care-gamification ("We know that the reality is the consumers don't read these contracts, or they do, but they have tremendous difficulty understanding them because they're written by lawyers for lawyers.").

[54] For an analysis of "clickwrap" agreements and court decision finding them enforceable, see Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 12 (2009) ("Generally such contracts, which are referred to as 'clickwrap' agreements, have been found enforceable if the online business can demonstrate the consumer has had reasonable notice of the terms and the consumer has assented to the terms."). However, a small number of courts have struck down select provisions of "clickwrap" agreements, like forum selection clauses, depending on the circumstances.

[55] *See e.g.*, *Fitbit Terms of Use*, FITBIT (Dec. 18, 2014), https://www.fitbit.com/terms ("[Users] grant to Fitbit a non-exclusive, transferable, sublicensable, worldwide, royalty-free license to use, copy, modify, publicly display, publicly perform and distribute Your Content only in connection with operating and providing the Fitbit Service. You are responsible for Your Content. You represent and warrant that you own Your Content or that you have all rights necessary to grant us a license to

policies governing the use of aggregated anonymous user data, data security and consumer responsibility for assisting in that security, and a precise listing of consumer information that is collected.[56] In combination, these terms and policies can give

---

use Your Content as described in these Terms."); *see also Jawbone Terms of Use*, JAWBONE (Dec. 16, 2014), https://jawbone.com/legal/terms ("IN NO EVENT SHALL JAWBONE AND/OR ITS SUPPLIERS OR LICENSORS BE LIABLE FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF USE, DATA OR PROFITS, ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE SITE(S), THE USE OR PERFORMANCE OF THE SITE(S), THE DELAY OR INABILITY TO USE THE SITE(S), OR FOR ANY INFORMATION, THIRD PARTY CONTENT, YOUR APPLICATIONS, SUBMISSIONS OBTAINED THROUGH THE SITE(S), OR OTHERWISE ARISING OUT OF THE USE OF THE SITE(S), WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF JAWBONE OR ANY OF ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF DAMAGES, AND EVEN IF THE LIMITED REMEDIES PROVIDED HEREIN FAIL OF THEIR ESSENTIAL PURPOSE. IF YOU ARE DISSATISFIED WITH ANY PORTION OF THE SITE(S), OR WITH ANY OF THESE TERMS, YOUR SOLE AND EXCLUSIVE REMEDY IS TO DISCONTINUE USING THE SITE(S). THIS SOLE AND EXCLUSIVE REMEDY IS SEPARATE AND INDEPENDENT OF ANY OTHER PROVISION THAT LIMITS JAWBONE'S LIABILITY OR YOUR REMEDIES. NOTWITHSTANDING THE FOREGOING, IN NO EVENT WILL JAWBONE'S AND/OR ITS SUPPLIERS OR LICENSORS TOTAL CUMULATIVE LIABILITY TO ANY THIRD PARTY FOR ALL DAMAGES, LOSSES AND CAUSES OF ACTION (WHETHER IN CONTRACT, TORT, INCLUDING NEGLIGENCE AND STRICT LIABILITY, OR OTHERWISE) EXCEED FIFTY U.S. DOLLARS (USD $50)).").

[56] *See Fitbit Privacy Policy*, FITBIT (Dec. 9, 2014), https://www.fitbit.com/privacy ("Fitbit may disclose non-personally identifiable aggregated user data, such as aggregated gender, age, height, weight, and usage data gathered from Fitbit devices (without the inclusion

insight into how a device maker may potentially utilize a user's CGLI and CGHI while limiting that user's legal recourse when he finally reads the fine print.

B. FDA authority over consumer health devices is limited to safety and effectiveness regulations rather than privacy

Compliance with FDA regulations is the first hurdle a consumer health device maker may need to clear depending upon the nature and classification of the device. The FDA's Center for Devices and Radiological Health ("CDRH") "is responsible for regulating firms who manufacture, repackage, relabel, and/or import medical devices sold in the United States."[57] While CGLI-monitoring devices will not likely qualify as "medical devices" under FDA regulations,[58] CGHI-

---

of a user's name or other identifying information) to: Organizations approved by Fitbit that conduct consumer research into health and wellness; Users of the Service for purposes of comparison of their personal health and wellness situation relative to the broader community; and Advertisers and other third parties for their marketing and promotional purposes."); *see also Jawbone Privacy Policy*, JAWBONE (Dec. 16, 2014) https://jawbone.com/legal/privacy (describing Jawbone's collection of demographic information, height, weight, and date of birth, detailed physical information including sleep cycle and activity intensity and duration, and precise location).

[57] *Medical Devices: Overview of Device Regulation*, FDA, http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/default.htm (last updated June 6, 2014).

[58] Draft guidance released by the FDA on January 20, 2015, states that the FDA "does not intend to examine low risk general wellness products to determine whether they are [medical] devices." The draft guidance divides general wellness products into two categories: first, products that have an intended use relating to "maintaining or encouraging a general state of health or a healthy activity"; and second, products that have an intended use to "promote, track, and/or encourage choice(s), which, as part of a healthy

monitoring devices will most likely be classified as "Class II medical devices" because of the nature of the information being monitored.[59]

FDA regulations generally require device makers initially to register their businesses, list their medical devices, and notify the market.[60] Device makers must follow quality control and good manufacturing processes when developing their devices, and it is the responsibility of "each manufacturer to establish and maintain a quality system that is appropriate for the specific medical device(s) designed or manufactured, and that meets the requirements of this part."[61] Device labels

---

lifestyle, [reduce the risk of or help live well with] certain chronic diseases or conditions." General Wellness: Policy for Low Risk Devices Draft Guidance for Industry and Food and Drug Administration Staff, 80 Fed. Reg. 2712 (Jan. 20, 2015), https://www.federalregister.gov/articles/2015/01/20/2015-00756/general-wellness-policy-for-low-risk-devices-draft-guidance-for-industry-and-food-and-drug.

[59] *See Is The Product A Medical Device?*, FDA (Sept. 12, 2014), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm (determining whether the FDA would classify a consumer health device as a "medical device"). *See, e.g.*, 21 C.F.R. § 870 (2013). As an example, "Cardiovascular Monitoring Devices" are enumerated under 21 C.F.R. § 870, Subpart C, and include devices that monitor oximetry, blood flow, and echocardiograph signals—information specifically monitored by the Scanadu Scout. *See* SCANADU, *supra* note 41. And more specifically, a "programmable diagnostic computer" is a Class II device defined under 21 C.F.R. § 870.1425 as a "a device that can be programmed to compute various physiologic or blood flow parameters based on the output from one or more electrodes, transducers, or measuring devices; this device includes any associated commercially supplied programs."

[60] 21 C.F.R. §§ 807.20, 807.81 (2013).

[61] 21 C.F.R. § 820.5 (2013); *Medical Devices: Quality System (QS) Regulation/Medical Device Good Manufacturing Practices*, FDA. (June 30, 2014), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/QualitySystemsRegulations/default.htm ("[This]

are also required to comply with FDA regulations and can include "written, printed, or graphic matter upon the immediate container of any [device]," as well as "posters, tags, pamphlets, circulars, booklets, brochures, instruction books, direction sheets, fillers, [and] labeling that is brought together with the device after shipment or delivery for shipment in interstate commerce."[62]

Once a device has been released to the public, device makers are required to monitor the safety and effectiveness of their devices; in the event of a device causing or contributing to a death or serious injury, the device maker must report such death or injury to the FDA.[63] Reports on devices may also contain complaints made to the FDA, which can include alleged "deficiencies related to the identity, quality, durability, reliability, safety, effectiveness, or performance of a device after it is released for distribution."[64]

---

regulation provides the framework that all manufacturers must follow by requiring that manufacturers develop and follow procedures and fill in the details that are appropriate to a given device according to the current state-of-the-art manufacturing for that specific device. . . . [This] regulation applies to finished device manufacturers who intend to commercially distribute medical devices. A finished device is defined in 21 CFR 820.3(l) as any device or accessory to any device that is suitable for use or capable of functioning, whether or not it is packaged, labeled, or sterilized.").

[62] *Medical Devices: Device Labeling*, FDA (June 30, 2014), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/DeviceLabeling/default.htm; *see also* 21 C.F.R. § 801 (2013) (Covers General Device Labeling); 21 C.F.R. §1010 (2013) (Covers General Electric Products).

[63] 21 C.F.R. §§ 803, 850–58 (2013) (regulating Medical Device Reporting).

[64] 21 C.F.R. § 820.3 (2013); *see also Medical Devices: Mandatory Reporting Requirements: Manufacturers, Importers and Device User Facilities*, FDA (Jan. 13, 2015), http://www.fda.gov/MedicalDevices/

The FDA does not limit its regulatory focus to only medical devices used by traditional medical providers, and the agency recently released its "Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff."[65] The FDA "encourages the development of mobile medical apps that improve health care and provide consumers and health care professionals with valuable health information."[66] The FDA, however, "also has a public health responsibility to oversee the safety and effectiveness of medical devices – including mobile medical apps."[67] CGLI-monitoring devices could eventually fall into this category of "medical device" as a result of the collected information being transmitted, automatically or manually, to device maker or third-party "apps."

DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/default.htm.

[65] *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff*, FDA, http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf (last visited Mar. 4, 2014). For a discussion of FDA regulation of the increasing use of smartphones and applications as medical devices, see Alex Krouse, *iPads, iPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications As Medical Devices*, 9 IND. HEALTH L. REV. 731 (2012).

[66] Importantly, "[m]obile applications (apps) can help people manage their own health and wellness, promote healthy living, and gain access to useful information when and where they need it. These tools are being adopted almost as quickly as they can be developed. According to industry estimates, 500 million smartphone users worldwide will be using a health care application by 2015, and by 2018, 50 percent of the more than 3.4 billion smartphone and tablet users will have downloaded mobile health applications." *Medical Devices: Mobile Medical Applications*, FDA, http://www.fda.gov/medicaldevices/productsandmedicalprocedures/connectedhealth/mobilemedicalapplications/default.htm (last visited Mar. 4, 2014).

[67] *Id.*

The FDA's regulatory power over mobile health ("mHealth") will not go unnoticed by the industry[68] despite the FDA "taking a limited regulatory approach to mobile health technologies [that] reflects the understanding that the market and the technology are relatively new."[69] But existing regulations largely focus on device safety and operability and do not include consumer privacy concerns. Despite this fact, consumer health device makers will certainly keep in mind FDA regulations as they drive the industry forward.[70]

---

[68] Tatiana Melnik, *There's an App for That! The FDA Offers A Framework for Regulating Mobile Health Those in the Health Care Space Should Expect the Mhealth Market to Continue to Grow*, 13 J. HEALTH CARE COMPLIANCE 45, 46 (2011) (stating that revenue from digital health technology and services in the United States is expected to "exceed $5.7 billion in 2015, compared with $1.7 billion in 2010, fueled by devices that monitor chronic conditions like hypertension and diabetes and by wellness and fitness applications and programs").

[69] *Id.* at 46, 65. The article is split between two sections, for the purposes of our article p. 46 is directly before 65.

[70] For a discussion on the issues that can arise when maintaining mobile medical applications in light of FDA regulations, see Williams, Kristy, *Updates are Not Available: FDA Regulations Deter Manufacturers from Quickly and Effectively Responding to Software Problems Rendering Medical Devices Vulnerable to Malware and Cybersecurity Threats*, 14 WAKE FOREST J. BUS. & INTELL. PROP. 367, 370 (2014) ("When a manufacturer discovers a software vulnerability in its medical device, the manufacturer is not necessarily obligated to remedy the vulnerability. Such vulnerabilities are primarily addressed through the issuance of software updates; however, a software update is considered a change in the medical device, and therefore must be evaluated to determine what obligations the manufacturer has under FDA regulations, including whether further FDA involvement is required."); *see also* Stacey Higginbotham, *Scanadu scores $10.5M and paves the way for FDA trials*, GIGAOM (Nov. 12, 2013, 7:00 AM), http://gigaom.com/2013/11/12/scanadu-scores-10-5m-and-paves-the-way-for-fda-trials (statement of Scanadu's CEO explaining the decision to seek FDA approval) ("We have chosen to go full FDA because we believe

C. HIPAA is applicable only to covered entities collecting protected health information

Consumer health information is regulated by HHS primarily through HIPAA.[71] Entities subject to HIPAA—"covered entities"—are traditional medical providers involved in holding, collecting, or transmitting protected health information.[72] Protected health information ("PHI") is defined under HIPAA as "individually identifiable health information: . . . that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium."[73] Individually identifiable health information derives from a subset of "health information," and includes demographic information collected from an individual *that is created or received by* a covered entity and relates to any physical or mental health or condition of an individual, or the provision of health care to an individual.[74] Consequently, until health information—no matter how sensitive the nature of that health information—is in the possession of a covered entity, it is not protected by HIPAA.[75]

---

consumers have the right to their own medical data and the right to accurate data.").

[71] 45 C.F.R. § 160, et seq. (2013).

[72] Covered entity under HIPAA is defined as "(1) A health plan; (2) A health care clearinghouse; (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." 45 C.F.R. § 160.103.

[73] *Id.*

[74] *Id.* (emphasis added) ("Individually identifiable health information also includes any payment for an individual's health care that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.").

[75] 45 C.F.R. § 160.103, *supra* note 10.

Entities governed by HIPAA must abide by the HIPAA Privacy Rule,[76] HIPAA Security Rule,[77] and HIPAA Breach Notification Rule.[78] Covered entities are not completely forbidden, however, from using the multitude of health information in their possession; covered entities are allowed to use protected health information as long as it is "de-identified."[79] De-identification allows companies utilizing health information to "facilitate beneficial studies that combine large, complex data sets from multiple sources."[80] De-identification involves removing "identifiers" from the health information, thereby minimizing privacy risks and supporting "the secondary use of data for comparative effectiveness studies, policy assessment, life sciences research, and other endeavors."[81] Nevertheless, even if a company attempts to protect individuals' data by de-identifying it, those measures

[76] 45 C.F.R. §§ 164.500-164.534 ("Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.").
[77] 45 C.F.R. §§ 164.302–164.318 ("A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.").
[78] 45 C.F.R. §§ 164.400–164.414 ("The requirements of this subpart shall apply with respect to breaches of protected health information.").
[79] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, HHS, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html (last visited Mar. 3, 2014).
[80] *Id.*
[81] *Id.*

may not be enough and the "de-identified" data may in fact be used to identify the individuals to whom it corresponds.[82]

D. The FTC has the authority to protect and define consumer privacy expectations

The FTC is yet another federal agency that can exert regulatory authority over the consumer health device industry.[83] The FTC has enforced companies' privacy policies for over fifteen years, resulting in broad influence over information privacy in the United States through the development of norms, best practices, and baseline privacy protections.[84] When a company suffers a breach of consumer data, politicians quickly turn to the FTC in order to determine if the company suffering the breach adequately protected its consumers' private information.[85] "When companies tell

---

[82] *See* Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117, 1122 (2013) (discussing the dichotomous view of "anonymous" data as a privacy matter or as a utility, including how even anonymized data can carry the potential to be used to identify the generating individual).

[83] The FTC has, in fact, begun taking a proactive interest in the consumer health-monitoring industry; for example, the FTC "been meeting with Apple as it looks to ensure that private health data collected by the company's phones, tablets, and upcoming smartwatch aren't used without their owners' consent." Jacob Kastrenakes, *FTC reportedly interested in privacy of Apple Watch health data*, THE VERGE (Nov. 13, 2004), http://www.theverge.com/2014/11/13/7217041/apple-ftc-reportedly-speaking-about-health-data-privacy.

[84] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586 (2014).

[85] *See* Julian Hattem, *Senators request probe of Home Depot hack*, THE HILL (Sept. 9, 2014 3:16 PM), http://thehill.com/policy/technology/217138-senate-dems-call-for-investigation-into-home-depot-hack (stating that only one day after a massive data breach at Home Depot was confirmed, two

consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises."[86]

The FTC's authority to regulate privacy derives primarily from Section 5 of the FTC Act.[87] The FTC also has authority over the regulation of consumer health information from other enabling legislation, such as the Health Information Technology ("HITECH") provisions of the American Recovery and Reinvestment Act of 2009.[88] Additional FTC authority to

---

Senators requested that the FTC investigate whether the company took appropriate measures to protect its consumers' private information).

[86] *Enforcing Privacy Promises*, FTC, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Apr. 7, 2014) (providing a number of FTC press releases, including, for example, an FTC enforcement action against Fandango, announced on March 28,2014, for misrepresenting the security of its mobile apps).

[87] 15 U.S.C. § 45 (2013), *available at* http://www.ftc.gov/enforcement/statutes/federal-trade-commission-act (last visited Mar. 4, 2014) ("Under this Act, the Commission is empowered, among other things, to (a) prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress.").

[88] For example, enabling legislation in the HITECH provisions of the American Recovery and Reinvestment Act of 2009 directed the FTC to issue a rule requiring entities that fall outside of HIPAA to notify individuals and the FTC when there is a "data breach or inadvertent disclosure of unsecured identifiable health information in personal health records." 42 U.S.C. §§ 17937, 17954 (2013); Health Information Technology ("HITECH") Provisions of American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D, FTC, available at

regulate data security and consumer privacy issues can be found in "narrower authority under sector-specific data security laws including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act of 1996 ("COPPA")."[89] One such rule is the Health Breach Notification Rule, which supplements HIPAA by requiring companies that store and provide access to consumer electronic personal health records ("PHRs") to contact customers in the event of a security breach.[90] Under the Rule, a consumer must be notified of a breach of "PHR identifiable health information" only if it is "*created or received by* a health care provider, health plan, employer, or health care clearinghouse."[91] When issuing the final Rule, the FTC also made note of comments suggesting that it establish "comprehensive privacy and security standards, and . . . [create] a private right of action for a violation of these standards," despite such action being outside the scope of the Rule.[92]

---

http://www.ftc.gov/enforcement/statutes/health-information-technology-hitech-provisions-american-recovery-and (last visited Mar. 4, 2014).

[89] Anne Marie Helm & Daniel Georgatos, *Privacy and mHealth: How Mobile Health 'Apps' Fit into a Privacy Framework Not Limited to HIPAA* (May 7, 2014). 64 SYRACUSE L. REV. 131, 159 (2014); UC Hastings Research Paper No. 108. Available at SSRN: http://ssrn.com/abstract=2465131.

[90] 16 C.F.R. § 318 (2013); *Health Breach Notification Rule*, FTC, http://www.business.ftc.gov/privacy-and-security/health-privacy/health-breach-notification-rule (last visited Mar. 4, 2014) (stating that in the event of a breach, companies must "Notify everyone whose information was breached; In many cases, notify the media; and notify the FTC").

[91] Health Breach Notification Rule; Final Rule, 74 Fed. Reg. 42962, 42968 (Aug. 25, 2009) (to be codified as 16 C.F.R. § 318) (emphasis added).

[92] *Id.* at 42963.

The FTC primarily protects a consumer's privacy interests in his health information through enforcement actions that can serve to bolster a prosecution under HIPAA or fill in the gaps where HIPAA may not be applicable or enforceable. A recent example of the FTC asserting its authority in this way is the FTC's enforcement action against LabMD for a breach of patient information.[93] The cancer-detection provider had argued that the FTC did not have the authority to take enforcement action because it is a covered entity under HIPAA; however, the FTC stated that "its enforcement authority under the FTC Act doesn't conflict with the Health and Human Services Department's regulation of health information data security practices under HIPAA."[94] The FTC posited that its ability to enforce data security policies under the FTC Act bolsters—rather than conflicts with—HIPAA, and that "so long as the requirements of those statutes do not conflict with one another, a party cannot plausibly assert that, because it complies with one of these laws, it is free to violate the other."[95] Ultimately, the FTC rejected LabMD's argument that the commission could not "bring an enforcement action without first issuing regulations detailing companies' data security obligations."[96] LabMD is not alone, however, in its

---

[93] *See FTC Affirms Data Security Enforcement Authority in Rejecting LabMD Arguments*, Health Law Reporter (BNA), 23 HLR Issue No. 5, pp. 155–56 (Jan. 30, 2014).

[94] *Id.*

[95] *Id.*

[96] *Id.* LadMD appealed the FTC's order denying its argument to the United States District Court for the Northern District of Georgia, but the appeal was dismissed on procedural grounds for lack of subject-matter jurisdiction because the FTC's order was not a final agency action. The District Court's dismissal was subsequently affirmed by the United States Court of Appeals for the Eleventh Circuit. LabMD, Inc. v. Federal Trade Commission, No. 14-12144 (11th Cir. Jan. 20, 2015).

criticism of the FTC's role in regulating new technologies, and critics of the FTC often take particular issue with the expansive use of Section 5 authority to regulate the area of consumer privacy in new technological industries.[97]

General protections for a consumer's lifestyle and health information can be found in a selection of sources (e.g., company privacy agreements, HIPAA regulations, and FTC enforcement actions). Some of these potential protections are inapplicable or insufficient; however, others could prove to protect consumer information while effectively defining consumer privacy expectations.

IV. REGULATION OF CONSUMER HEALTH DEVICE MAKERS SHOULD BE PURSUED WHILE BALANCING THE NEED FOR INNOVATION WITH THE STRICTURES OF REGULATORY COMPLIANCE

Protecting privacy is often viewed as being of the utmost importance with some theorists viewing privacy "as a basic human good or right with intrinsic value" that is "an essential component of human well-being."[98] A more common view, however, "is that privacy is valuable because it facilitates or promotes other fundamental values, including ideals of

---

[97] *See, e.g.*, Geoffrey A. Manne, *Humility, Institutional Constraints & Economic Rigor: Limiting the FTC's Consumer Protection Discretion* INTERNATIONAL CENTER FOR LAW & ECONOMICS (ICLE), Working Paper 2014-1, July 31, 2014. *available at* http://ssrn.com/abstract=2474523 (critically discussing the FTC's decision-making in consumer protection enforcement actions).

[98] SHARYL J. NASS ET AL., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 77 (2009), *available at* http://www.ncbi.nlm.nih.gov/books/NBK9579.

personhood . . . such as: Personal autonomy (the ability to make personal decisions), Individuality, Respect, [and] Dignity and worth as human beings."[99] The importance of protecting private, consumer-generated lifestyle and health information cannot be understated; in fact, "[t]here is nothing more sensitive than your medical data."[100]

Despite a premium being placed on privacy, the legal protections in place to protect consumer privacy expectations have not kept up with the pace of technological change.[101] Moore's Law is generally accepted as the proper measurement of technological change in an industry.[102] Moore's Law posits that the rate of improvement for a technology increases at an exponential level; however, there are variances in this rate depending on the technology.[103] Another law, Wright's Law, posits "that progress increases with experience — specifically, that each percent increase in cumulative production in a given

---

[99] *Id.*

[100] Ashley Gold, *Accompanying Apple Watch, a medical surprise*, POLITICO (Mar. 9, 2015), http://www.politico.com/story/2015/03/apples-researchkit-wants-to-change-traditional-medical-research-115918.html (quoting Jeff Williams, Apple's senior vice president of operations, during an announcement of the company's Healthkit apps which allow iPhone users to test themselves for certain diseases without visiting a doctor's office).

[101] Privacy laws lagging behind technological change is not a new trend. In fact, technological advances have often served as the catalyst for change in privacy law: "Whether [privacy] concerns implicated the government or the private sector, the driving force behind them was technological change that threatened the security of individuals' information and allowed for increasingly sophisticated analysis and use of that information." Helm & Georgatos, *supra* note 89, at 141.

[102] David L. Chandler, *How to predict the progress of technology*, MITNEWS (Mar. 6, 2013), http://web.mit.edu/newsoffice/2013/how-to-predict-the-progress-of-technology-0306.html.

[103] *Id.*

industry results in a fixed percentage improvement in production efficiency."[104] Taken together, these laws indicate that the CGLI and CGHI-monitoring industry will develop quickly in both the accuracy and quality of information collected as well as the ability to collect, analyze, and make use of the information.

A. Past consumer data breaches show the need for protection of CGLI and CGHI, despite the potential regulatory costs to the consumer health device industry

CGLI and CGHI monitoring can aggregate a consumer's health information across a number of different devices, apps, and services, can assist that consumer in diagnosing his own health, and can provide a quick and easy way to transmit the consumer's health information to a health care provider when necessary. But the risks for a consumer could outweigh the rewards as the industry continues to develop. The progression of data privacy laws, as well as the data breaches and consumer concerns that have spurred changes in those laws,[105] demonstrate that it is a far better course of action to require consumer health device makers to be at the forefront of consumer information protection rather

---

[104] *Id.*

[105] For example, a history of technological advancement demonstrates the areas in which consumers are more likely to demand, rather than forego, privacy protections when adopting technology to their lifestyle. *See, e.g.*, Helm & Georgatos, *supra* note 89, at 141–46 (discussing the trade-off between privacy and convenience in the development of communications technologies and the use of big data by the credit industry).

than wait for a catastrophic event to spur action by a company, the market in general, or Congress.[106]

A recent, widely-publicized data security breach highlights the fact that preventive, rather than reactive, measures are more desirable for both companies and consumers alike. Credit card companies and retailers in the United States have lagged behind Europe in utilizing "chip and pin" technology to protect consumer credit and debit cards; however, following the massive Target retail store data breach in November and December of 2013, an industry-wide effort began to adopt this higher level of protection for consumers.[107] Target also failed to inform customers of the breach until weeks after its occurrence, and legislation was quickly proposed to penalize companies for failing to notify customers when a breach of customer data had occurred.[108] The Target data breach was a failure on many levels and emphasized that relying on a company to self-report out of its own "good will"

---

[106] "Health information, [like personal communications and other private consumer information], has long been recognized as deserving special privacy protections." *Id.* at 147.

[107] Target is on track to upgrade every store to chip and pin technology—a more sophisticated method to authenticate a purchase than the magnetic strip and signature method currently in use—in the United States by September of 2014. Newly named Chief Information Officer, Bob DeRodes, recognized the need for quick action, proclaiming "I think of the payment industry as an arms race, where retailers and banks have to stay out ahead of the bad guys." Sam Machkovech, *Stung by data breach, Target speeds switch to chip-and-PIN card readers*, ARS TECHNICA (Apr. 29, 2014), http://arstechnica.com/information-technology/2014/04/stung-by-data-breach-target-speeds-switch-to-chip-and-pin-card-readers.

[108] Rebecca Lopes, *Target's data breach leaves customers fearful of future privacy invasions*, CAMPBELL LAW OBSERVER (Jan. 21, 2014), http://campbelllawobserver.com/2014/01/targets-data-breach-leaves-customers-fearful-of-future-privacy-invasions.

is not a viable solution when the costs of disclosure—not only to the financial bottom line but also to the executives at the top[109]—can be incredibly high, thereby outweighing any incentives behind self-reporting. In fact, a consumer is typically the last to know of a breach of his personal information.[110]

Malicious attempts by third parties to access consumer information are not the only potential source for a breach of consumer information, and a consumer health device user could unintentionally breach his own CGLI or CGHI. For instance, a user could resell his device but either fail to deactivate or improperly deactivate that device from the information-monitoring service. When the device's new user subsequently syncs the information collected by the device, it

---

[109] Target is suffering financially for failing to properly protect its consumers' data, and has announced that it will invest over $100 million in upgrading technology and providing remedial measures for its affected customers. Mark Calvey, *Target security breach accelerates adoption of chip-and-pin cards*, SAN FRANCISCO BUS. TIMES (Feb. 4, 2014), http://www.bizjournals.com/sanfrancisco/blog/2014/02/target-visa-mastercard-senate-hearing.html; Anne D'Innocenzio, *Target's 4Q profit drops 46 pct on costs related to massive data breach*, ASSOCIATED PRESS (Feb. 26, 2014), http://www.usnews.com/news/business/articles/2014/02/26/data-breach-costs-take-toll-on-target-profit ("The nation's second largest discounter said Wednesday that its profit in the fourth quarter fell 46 percent on a revenue decline of 5.3 percent as the breach scared off customers worried about the security of their private data."); Russell Brandom, *Target CEO resigns in the wake of data breach*, THE VERGE (May 5, 2014), http://www.theverge.com/2014/5/5/5682810/target-ceo-resigns-in-the-wake-of-data-breach (explaining that Target's CEO Gregg Steinhafel, as well as the company's chief technology officer, resigned only a few short months following the massive breach).

[110] *See* Craig Timberg et al., *Hacked? Customers are often last to know*, WASH. POST (Aug. 28, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/28/hacked-customers-are-often-last-to-know.

could potentially be transmitted to the original user's service profile or other connected services.[111] Such an example is not far from reality, as iPhone users in 2011 experienced a similar situation with iMessages being sent to both the original and new owner's iPhones.[112]

Likewise, the device maker could unintentionally breach its users' CGLI or CGHI when it chooses to utilize or sell consumer information—even when that information has been de-identified. Netflix and AOL, for example, are two companies that chose to de-identify user information to facilitate studies while also unintentionally presenting researchers the opportunity to "re-identify" the users.[113] Following the disclosures, studies showed that "re-identification can occur even by combining non-[personally identifiable information], such as movie ratings in the Netflix study or search engine queries in the AOL example."[114] Both companies received a great deal of negative attention despite each having good intentions in using the "anonymized customer data."[115] A similar potential for unintentional disclosure in the CGLI-monitoring industry already exists, as

---

[111] *See, e.g.*, *supra* Part I.a (describing fitness tracker sync services).

[112] Jacqui Cheng, *Stolen iPhone? Your iMessages may still be going to the wrong place*, ARS TECHNICA (Dec. 14, 2011 4:50 PM), http://arstechnica.com/apple/2011/12/stolen-iphone-your-imessages-may-still-be-going-to-the-wrong-place.

[113] *Re-identification*, EPIC, http://epic.org/privacy/reidentification (last visited Apr. 14, 2014).

[114] *Id.*; *see also* Health Breach Notification Rule, 74 Fed. Reg. 42962, 42968 (noting empirical evidence and multiple studies that showed how data could be re-identified).

[115] David Coursey, *New "Irresponsible" Netflix Contest May Violate Customer Privacy*, PC WORLD (Sept. 22, 2009 9:57 AM), http://www.pcworld.com/article/172373/New_Irresponsible_Netflix_Contest_May_Violate_Customer_Privacy.html.

companies are already putting consumer information to public use.[116] Additionally, many data breaches often originate from employee access to the increasing amount of consumer information collected and stored by companies.[117]

Protecting the intimate and potentially embarrassing details in a consumer's health information is imperative, but adding protection for the consumer could also result in intense and expensive compliance for the device maker.[118] For example, compliance with HIPAA can prove to be a costly endeavor.[119] A 2013 survey of physicians, hospital administrators, and IT professionals found that "Fifty-one

---

[116] For example, RunKeeper, a smartphone app that can also sync with CGLI-monitoring devices like Fitbit, recently released user data collected by its app to show the most popular running routes in a number of cities. *See* Josh Lowensohn, *Blurred lines: data project shows popular running routes in 22 cities*, THE VERGE (Feb. 6, 2014 10:06 PM), http://www.theverge.com/2014/2/6/5388346/blurred-lines-data-project-shows-popular-running-routes-in-22-cities ; *see also* Monica Laliberte, *For secretive companies, your health data means big money*, WRAL (May 19, 2014), http://www.wral.com/for-secretive-companies-your-health-data-means-big-money/13656317/ (discussing data mining companies and how those companies utilize consumer health information sold by various online and retail businesses).

[117] Andrea Peterson, *When cybersecurity threats come from the inside*, WASH. POST (Oct. 8, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/08/when-cybersecurity-threats-come-from-the-inside.

[118] *See* Stacey Higginbotham, *Scanadu scores $10.5M and paves the way for FDA trials*, GIGAOM (Nov. 12, 2013 7:00 AM), http://gigaom.com/2013/11/12/scanadu-scores-10-5m-and-paves-the-way-for-fda-trials (noting that Scanadu's decision to seek full FDA approval before going to market has resulted in its public release of the Scanadu Scout being pushed back to the end of 2014 at the very earliest).

[119] Lucas Mearian, *HIPAA rules, outdated tech cost U.S. hospitals $8.3B a year*, COMPUTERWORLD (May 7, 2013), http://www.computerworld.com/s/article/9238954/HIPAA_rules_outdated_tech_cost_U.S._hospitals_8.3B_a_year.

percent of respondents say HIPAA compliance requirements can be a barrier to providing effective patient care. Specifically, HIPAA reduces time available for patient care (according to 85% of respondents), makes access to electronic patient information difficult (79%) and restricts the use of electronic communications (56%)."[120]

The following sections analyze potential solutions for the protection of CGLI and CGHI. Section (b) examines the possibility of leaving protection to the *status quo* by allowing the market to continue to self-regulate. Section (c) discusses how existing HHS regulations like HIPAA do not currently cover consumer health device makers and then analyzes the feasibility of expanding the definition of covered entities to encompass consumer health device makers. Section (d) examines FTC specialization in protecting consumer interests and posits that the FTC, as the ideal agency to regulate privacy concerns with consumer health devices, should utilize a two-pronged approach to regulate consumer health device makers effectively and protect consumers.

B. Maintaining the *status quo* by leaving consumer protection to the market is an insufficient solution

The argument could be made that maintaining the *status quo* is perfectly acceptable, and that consumers would shift away from a company that improperly uses, abuses, or otherwise fails to protect its users' personal information. The market could determine what is an appropriate measure of privacy protection while a consumer would be free to decide if he even desires for his health information to be protected and, if so, what level of protection is enough to satisfy his needs.

---

[120] *Id.*

Devices like Fitbit currently collect only a limited set of CGLI and in a consumer's eyes might require less privacy protection than a device like the Scanadu Scout that collects CGHI. But as the Fitbit sexual activity example demonstrates, even the tiniest of details about a user's personal habits could prove to be incredibly sensitive information.[121]

Consumers frequently demonstrate that they are incapable of making the decision to shift away from a popular company that fails to protect its users' information.[122] For example, social media giant Facebook has continued its march to "the next billion" users despite settling with the FTC on charges that it "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."[123] Search engine powerhouse Google continues to grow despite paying millions of dollars in fines after settling with the FTC for misrepresenting to users of Apple's Safari web browser "that it would not place tracking 'cookies' or serve targeted ads to those users, violating an earlier privacy settlement between

---

[121] Kashmir Hill, *Fitbit Moves Quickly After Users' Sex Stats Exposed*, FORBES (July 5, 2011 7:58 AM), http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed.

[122] And if a service is truly viewed as necessary by a consumer, he may be *unable to* shift away.

[123] *FTC Approves Final Settlement With Facebook*, FTC (Aug. 10, 2012), http://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook ("The settlement requires Facebook to take several steps to make sure it lives up to its promises in the future, including by giving consumers clear and prominent notice and obtaining their express consent before sharing their information beyond their privacy settings, by maintaining a comprehensive privacy program to protect consumers' information, and by obtaining biennial privacy audits from an independent third party.").

the company and the FTC."[124] Fledgling social network Path is still going strong, even after it settled with the FTC for deceiving its mobile app users into allowing the collection of personal information without the users' knowledge.[125] And credit cards from Visa and MasterCard remain the most popular options for consumers despite the data from thousands of customers being breached by a subsidiary in 2012.[126]

Similarly, consumer trust in consumer health device makers could also prove blinding. A study released in January of 2013, conducted by Ponemon Institute and sponsored by computer security company Symantec, found that healthcare and consumer products industries were considered by consumers to be among the most trusted for privacy among

---

[124] *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FTC (Aug. 9, 2012), http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented ("The settlement is part of the FTC's ongoing efforts make sure companies live up to the privacy promises they make to consumers, and is the largest penalty the agency has ever obtained for a violation of a Commission order.").

[125] *Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books*, FTC (Feb. 1, 2013), http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived ("[The FTC charged that Path's app] was misleading and provided consumers no meaningful choice regarding the collection of their personal information."). Path agreed to pay $800,000 to settle the charges, and FTC Chairman Jon Leibowitz proclaimed that "This settlement with Path shows that no matter what new technologies emerge, the agency will continue to safeguard the privacy of Americans." *Id.*

[126] Alex Fitzpatrick, *Got Visa or Mastercard? Your Data May Have Leaked*, MASHABLE (Mar. 30, 2012), http://mashable.com/2012/03/30/credit-card-leak.

twenty-five different industry categories.[127] This trust comes in spite of healthcare-related companies regularly suffering data breaches, some of which affect millions of consumers.[128] The study, however, also highlighted consumers' somewhat conflicting privacy expectations. The study found that seventy-eight percent of respondents perceived privacy and the protection of their personal information as very important or important to the overall trust equation, a percentage that was trending up; nevertheless, the study also found that sixty-three percent of respondents admitted to sharing their sensitive personal information with an organization they did not know or trust.[129] Notably, thirty-two percent of respondents admitted

---

[127] *2012 Most Trusted Companies for Privacy*, PONEMON INST., 1 (Jan. 28, 2013), http://www.ponemon.org/local/upload/file/2012%20MTC%20Report%20FINAL.pdf.

[128] For example, the personal information for almost five million Tricare military beneficiaries was breached in 2011 in "one of the largest health-data breaches ever reported." Steve Vogel, *Tricare military beneficiaries being informed of stolen personal data*, WASH. POST (Nov. 24, 2011), *available at* http://www.washingtonpost.com/politics/tricare-military-beneficiaries-being-informed-of-stolen-personal-data/2011/11/23/gIQAcRNHtN_story.html; *see also* Elise Viebeck, *Chinese hackers stole data of 4.5M patients*, THE HILL (Aug. 8, 2014, 10:30 AM), http://thehill.com/policy/healthcare/215377-chinese-hackers-stole-patient-data-for-45m-hospital-chain-says ("Law enforcement had previously warned the U.S. healthcare sector that its systems were vulnerable to attacks seeking intellectual property and patient data.").

[129] *2012 Most Trusted Companies for Privacy*, *supra* note 127, at 1. Moreover, the paradox of consumers continuing to use services requiring the collection of private information despite maintaining a distrust of the service providers is emphasized by a pair of recent studies from Pew Research Center and the Centre for International Governance Innovation. *See* Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions; *see*

that they do not rely on privacy policies when judging the privacy practices of organizations, with sixty percent of those respondents believing that such policies are too long or contain too much legalese.[130]

Relying on consumer "groupthink" as the way to regulate company privacy policies and punish bad actors after a data breach is not a reliable option. Likewise, such reliance misses the point that preventing a breach of privacy *before it happens* is much more desirable than forcing consumers to rely on a lawsuit or public outcry *after the fact*. Consumers often click-through the terms of service for a device at a brisk pace in order to begin using the new gadget immediately,[131] failing to realize that those terms can significantly limit legal options in the future.[132] An oblivious consumer may not realize that by consenting to the terms he has, for example, agreed to allow a device maker to market his health information.[133] And if the user decides to challenge the company on its use of his information, he will typically be relegated to arbitration—a

---

also CIGI-Ipsos Global Survey on Internet Security and Trust, CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION, https://www.cigionline.org/internet-survey (last visited Jan. 11, 2015).

[130] *2012 Most Trusted Companies for Privacy*, *supra* note 127, at 1.

[131] For instance, "a 2006 UC Berkeley survey found that only 1.4 percent of participants read these sorts of agreements 'often and thoroughly,'" due in large part to the fact that it would take "more than 300 hours to read the privacy policy at the websites [an average consumer] visit[s] each year." James Temple, *Why privacy policies don't work—and what might*, SFGATE (Jan. 29, 2012, 4:00 AM), http://www.sfgate.com/business/article/Why-privacy-policies-don-t-work-and-what-might-2786252.php.

[132] Gindin, *supra* note 54.

[133] *See, e.g.*, *Fitbit terms of use*, *supra* note 55.

practice that is much more favorable to the company than it is to the consumer.[134]

There is, however, an important factor in favor of leaving the regulation of CGLI and CGHI privacy to the device makers themselves: the potentially high cost of regulatory compliance.[135] The increased economic cost of regulatory compliance for device makers would likely be passed through to the end user, resulting in a higher overall cost per device and detracting from one of the most appealing features of consumer devices—the low cost.[136] If a key selling point of CGLI-monitoring and CGHI-monitoring devices is minimized, it may result in fewer companies entering the market to begin with—decreasing competition and slowing innovation.[137] In addition, the danger of requiring device makers to warn consumers constantly about *potential* dangers could create an unfair perception that the devices simply are not trustworthy, thereby

---

[134] *See Searle Institute Report Shows Mandatory Arbitration Favors Corporations Over Consumers*, AM. ASS'N FOR JUST., *available at* https://uproxx.files.wordpress.com/2014/04/searle_arbitration_rebut.pdf (last visited Mar. 3, 2014) ("Business claimants win overwhelmingly more cases than consumers. Searle's data shows that consumers won some relief in 53.3% of cases they filed; however, business claimants won relief in 83.6% of cases.").

[135] For a discussion of costs and benefits of regulating Health Information Technology ("HIT"), see Daniel J. Gilman & James C. Cooper, *There Is A Time to Keep Silent and A Time to Speak, the Hard Part Is Knowing Which Is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279, 327–34 (2010).

[136] *Id.* at 328.

[137] *Id.* at 328 (explaining that in the context of a hospital and HIT adoption, "If consent requirements reduce HIT benefits, providers also will be less likely to adopt HIT in the first place. Some empirical evidence supports this hypothesis").

utterly damaging consumer confidence in the device makers and potentially deterring consumers from purchasing new consumer health devices.[138] This cost of compliance to the device maker, however, can be outweighed overwhelmingly by the financial cost of a data breach and the damage to a company's public image.[139]

Moreover, the benefits to consumers in holding companies accountable should outweigh a potential negative impact on the consumer health device industry.[140] For instance, proactive requirements can be established to incentivize the prevention of data breaches; and, if there is a breach, requiring consumer notification of that breach can set in motion prophylactic actions to minimize the damage.[141] Moreover, requiring a device maker to keep its users informed

---

[138] *Id.* at 331.

[139] *2013 Cost of Data Breach Study: Global Analysis*, PONEMON INST. (2013), https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf (finding that the average cost of a data breach for a company was $188 per user and the highest cost for a data breach was $5.4 million).

[140] For a comparable discussion weighing the costs and benefits of patient safety and market forces in light of FDA regulation of MHealth applications, see Daniel F. Schulke, *The Regulatory Arms Race: Mobile-Health Applications and Agency Posturing*, 93 B.U. L. REV. 1699, 1751 (2013) ("Ultimately, even though FDA approval is slow, given a simple choice between no regulation and regulation, patient safety should triumph over innovation in an industry. Innovation may produce new, more clinically effective applications that can improve the health of patients, but the potential harm to innovation caused by FDA regulation is a necessary evil. The marginal benefit created by applications being quicker to market is not worth the potentially severe and irreparable harm caused to the health of patients by error-ridden applications. No patient should suffer harm simply to allow an industry to be free to react faster to market changes.").

[141] Gilman & Cooper, *supra* note 135, at 329.

could ensure that a consumer will be as knowledgeable about his own lifestyle and health information as he is in how that information is being protected and used by the device maker.[142]

Furthermore, the ability of consumers to hold consumer health device makers accountable—under a claim for breach of contract—in the event of a breach of that company's privacy policy is tenuous at best.[143] If a consumer were able to rely only on a lawsuit against a device maker for mishandling his lifestyle and health information, he would essentially be helpless.[144] Efficient regulatory oversight is therefore unmistakably needed to ensure that CGLI and CGHI are

---

[142] *Id.* at 330 ("According to some commentators, consumers have a basic right to privacy that includes being informed when their personal information has been compromised."); The degree of what constitutes an actual "notification-worthy" breach of CGHI will also need to be determined. Leaving the decision to the device makers of what breach is "notification-worthy" would give them too much latitude; device makers would most likely err on the side of *not* notifying consumers because of the financial costs of a breach. *2013 Cost of Data Breach Study: Global Analysis*, PONEMON INST (2013), *supra* note 139. The threshold level of what breach is notification-worthy will require a balance be struck between informing consumers of every "negligible" breach, which would likely be counterproductive, and informing consumers of only drastic "newsworthy" data breaches, which would be far too limiting. One option that should be considered is to define various levels of breaches that result in corresponding degrees of notification, i.e., the greater the breach the more detailed the notification. The Health Breach Notification Rule could also be utilized in developing notification standards for the industry. Health Breach Notification Rule; Final Rule, 74 Fed. Reg. 42962, 42968 (Aug. 25, 2009) (to be codified as 16 C.F.R. § 318) (emphasis added).

[143] For a discussion of the weaknesses in relying on privacy policies and breach of contract claims, *see* Solove & Hartzog, *supra* note 84, at 597–99.

[144] *Id.*

properly protected as the consumer health device industry continues its explosive growth.[145]

C. Expanding HIPAA's definition of covered entities to include consumer health device makers would prove too unwieldy a solution

One way to regulate consumer health device makers would be through changes to HHS authority under HIPAA. A specific change to the definition of "covered entities" could be made to include consumer health device makers. Currently, only one of the three types of entities deemed a covered entity—health care providers that transmit health information electronically—could potentially include CGHI-monitoring device makers; however, it would require an etymological stretch to additionally include CGLI-monitoring device makers, like Fitbit, in the same category as the traditional "health care providers" originally envisioned under HIPAA.[146] Consequently, there is no present authority for HHS to enforce HIPAA compliance by consumer health device makers directly, and a new standard governing consumer interactions

---

[145] Gindin, *supra* note 54 (discussing the dangers in consumers relying on company privacy policies and terms of service for privacy protections).

[146] For instance, when the Notice of Proposed Rulemaking for HIPAA was announced, HHS stated that the definition of a "health care provider" would include "a researcher who provides health care to the subjects of research, free clinics, and a health clinic or licensed health care professional located at a school or business . . . [as well as] the Medicare definition of a provider, which encompasses institutional providers, such as hospitals, skilled nursing facilities, home health agencies, and comprehensive outpatient rehabilitation facilities." Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 45 Fed. Reg. 59918, 59930 (Nov. 3, 1999) (to be codified at 45 C.F.R. § 160.103).

with these device makers would be required.[147] An option more feasible than attempting to qualify a device maker into one of the three current types of covered entities would be that a fourth type of covered entity could be proposed expressly to include consumer health device makers. Yet this option would still face the obstacle of the rulemaking process and would not provide an immediate solution.[148] Importantly, an expansion of HIPAA compliance to consumer health device makers would result in an expansion of HIPAA into new ground beyond traditional medical providers.

Simply put, the only current way for HHS to regulate a consumer's CGLI or CGHI is if his information is transmitted to or held by a HIPAA-defined covered entity, thereby transforming that same information into PHI merely because it is now held by a traditional medical provider.[149] However, such a transmittal may never occur with consumer health devices. While these devices have been marketed as providing consumers with an easier way to convey specific lifestyle and health information to a physician, the devices are also marketed as a way to encourage self-diagnosis and self-treatment.[150]

---

[147] For a helpful chart on determining if an entity is a covered entity, *see Covered Entity Charts*, CENTERS FOR MEDICARE & MEDICAID SERVICES, *available at* http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/CoveredEntityCharts.pdf (last visited Mar. 3, 2014).

[148] *See, e.g.*, *Health Information Privacy: For Covered Entities and Business Associates*, *infra* note 152.

[149] *See Health Information Privacy: Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#protected (last visited Mar. 3, 2014).

[150] *See, e.g.*, SCANADU, *supra* note 40.

Moreover, protecting the consumer's information strictly because it has been transmitted *from the device* to a limited subset of health care providers fails to protect that same information while it remains, before *and* after the transfer, in the device or device maker's service.[151]

Significantly relying on any proposed change to HIPAA could be drastic, take years to implement, and would still leave consumers' lifestyle and health information unprotected in the meantime. The recent expansion of HIPAA's data protection requirements of covered entities to "business associates" demonstrates this reality in agency rulemaking: it can be years between proposal and implementation.[152] HHS Health IT policies already in place could help speed up the process and guide policy makers despite being primarily applicable to traditional healthcare providers.[153] But consumer devices are frequently updated with new features being added each year, and a certain level of

---

[151] The possibility does exist that a consumer health device maker could be a "business associate" of a covered entity, and accordingly be subject to HIPAA; however, such a situation will occur only if the device maker has a relationship with the covered entity in which it performs certain functions on behalf of or provides services to the covered entity. 45 C.F.R. § 160.103.

[152] For example, the recent changes to HIPAA were first proposed in July of 2010, adopted in January of 2013, and ultimately implemented in September of 2013. *See generally Health Information Privacy: For Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH AND HUM. SERVS, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities (last visited Mar. 3, 2014). The final rule is available at https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the.

[153] *See generally Privacy & Security Policy*, HEALTHIT.GOV, http://www.healthit.gov/policy-researchers-implementers/privacy-security-policy (last visited Mar. 3, 2014).

foresight would be necessary to anticipate just what these consumer health devices will be capable of doing years down the road. In sum, because HHS offers no immediate protection of consumer privacy expectations in CGLI or CGHI, HHS is not the ideal federal agency to regulate consumer health device makers despite that agency's current regulatory oversight over traditional healthcare entities. HHS could offer privacy protections in the future as consumer health devices become more sophisticated, but charging HHS with regulating *consumer* devices would be a drastic expansion of HIPAA outside of the traditional medical provider context and could lead to unintended collateral effects.[154]

Relying on device maker privacy policies is an inadequate solution and relying on a change to HIPAA would leave no solution for the immediate users of consumer health devices. Technological change—especially in a burgeoning industry like the consumer health device industry—will not come to a halt while regulators take years to implement new regulations. While CGLI-monitoring devices are unmistakably exploding in popularity,[155] CGHI-monitoring devices have not

---

[154] For example, the FTC's Red Flags Rule, initially issued in 2007, was thought to apply to traditional financial institutions and creditors; however, the Rule was interpreted in an expansive manner that included businesses well outside of the dictionary definition of "creditor." The unintended consequences of such an interpretation were remedied only after the rule was amended by the Red Flag Program Clarification Act of 2010. *Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business*, FTC (2013), http://business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business.

[155] Kelsey Pommer, *Digital Health and Fitness Tech is on the Move at 2014 CES*, DIGITAL DIALOGUE (Jan. 7, 2014), http://www.ce.org/Blog/Articles/2014/January/2014CES/Digital-Health-and-Fitness-Tech-is-on-the-Move-at.aspx ("In fact, a 2013 CEA survey found that one-third (33 percent) of

yet begun the inevitable flood *en masse* into the consumer market.[156] This dichotomous timeframe allows for the development of a two-pronged approach, both for CGLI-monitoring devices in the short term and CGHI-monitoring devices in the long term.

D. The FTC, to protect consumer privacy interests, should utilize its current enforcement authority to protect CGLI in the short term and develop needed rules governing CGHI protection in the long term

Rather than attempting to rely on ineffective individual lawsuits against device makers or currently inapplicable HIPAA regulations, the more desirable way of protecting consumers is through consumer-focused FTC enforcement actions in the short-term and targeted rulemaking in the long-term. Due to the nature of the information contained within CGLI, the FTC should equate CGLI-monitoring device makers with any other consumer device maker that stores or otherwise deals in sensitive consumer information. In other words, it should treat lifestyle information in the same manner as it treats credit card numbers, social security numbers, and the like. But because of the greater accuracy, complexity, and sensitivity of CGHI, the FTC will need to develop directed rules as CGHI-monitoring devices enter the consumer market and as the growing sophistication of CGLI-monitoring devices moves them closer to being considered CGHI-monitoring devices.

---

mobile device owners have used their devices to track some aspect of their health in the last 12 months.").

[156] *See, e.g.*, Higginbotham, *supra* note 70 (discussing Scanadu's widespread consumer release likely being pushed back many months due to its decision to seek full FDA approval).

The FTC is the best-equipped federal agency to pursue such a strategy for a number of reasons. Most notably, the FTC is already focused on protecting consumer privacy and security in the modern "Internet of Things"[157] world, even holding a workshop in November of 2013[158] to focus on the increasing interconnectedness of consumer devices—both at home and on the move—and releasing a staff report in January of 2015[159] largely summarizing the 2013 workshop and offering recommendations. FTC Commissioner Julie Brill discussed in November of 2014 the current applicability of FTC rules on privacy and security to the Internet of Things, but

---

[157] While the phrase is now ubiquitous in its use by consumer-focused technology companies, the phrase "Internet of Things" was likely coined in 1999 by Kevin Ashton, co-founder and former executive director of the Auto-ID Center. Kevin Ashton, *That 'Internet of Things' Thing*, RFID JOURNAL (June 22, 2009), http://www.rfidjournal.com/articles/view?4986.

[158] "The ability of everyday devices to communicate with each other and with people is becoming more prevalent and often is referred to as 'The Internet of Things.' Connected devices can communicate with consumers, transmit data back to companies, and compile data for third parties such as researchers, health care providers, or even other consumers, who can measure how their product usage compares with that of their neighbors." *Internet of Things - Privacy and Security in a Connected World*, FTC, http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world (last visited Mar. 4, 2014).

[159] The staff report focuses on three key areas in consumer protection for interconnected devices: security, data minimization, and notice and choice. The staff report noted that staff believes Internet of Things-specific legislation would be premature, but staff reiterated "the Commission's previous recommendation for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach." *Internet of Things FTC Staff Report*, FTC (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

also said she "does not currently see the need for new rulemaking."[160] While Commissioner Brill is correct in the sense that current FTC authority is applicable to consumer information, the sensitive nature of consumer-generated health information makes apparent the need for future agency action regarding its protection.[161]

1. Enforcement actions under the FTC Act should be utilized in the short-term to protect consumer privacy expectations in CGLI

The FTC "prides itself on its in-house technological skills and ability to keep up with evolving challenges" and despite its "relatively small size, . . . believes [it] has a significant influence through the enforcement actions it undertakes."[162] For example, the FTC's first enforcement action against an "Internet of Things" device maker, TRENDnet, could exemplify and foreshadow what an FTC enforcement action would look like against bad-actor device makers.[163] TRENDnet, while not a consumer health device maker, similarly dealt in sensitive consumer information and heightened privacy expectations: namely, live video feeds originating from inside a user's home.[164] The FTC alleged that TRENDnet had "failed to provide reasonable security to

---

[160] David McAuley, *FTC in Cyberspace: Ready, or Not, for Coming Wave of Connected Devices*, BLOOMBERG BNA (Nov. 20, 2014), http://www.bna.com/ftc-cyberspace-ready-n17179880248.
[161] *Infra*, Part III.d.ii.
[162] McAuley, *supra* note 160.
[163] *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy*, FTC, http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles (last visited Mar. 4, 2014).
[164] *Id.*

prevent unauthorized access to sensitive information, namely the live feeds from [users'] IP cameras," and as a result of this failure, hundreds of consumers' private camera feeds were made public on the Internet.[165] The terms of the resulting settlement between the FTC and TRENDnet are comprehensive, requiring TRENDnet to establish a security program to prevent such breaches in the future, to obtain third-party assessments of its security programs for the next twenty years, to notify customers of security issues, and to provide free support for two years to customers.[166] TRENDnet was also "prohibited from misrepresenting the security of its cameras or the security, privacy, confidentiality, or integrity of the information that its cameras or other devices transmit [and] is barred from misrepresenting the extent to which a consumer can control the security of information the cameras or other devices store, capture, access, or transmit."[167] The assertion of authority under Section 5 of the FTC Act over alleged unfair or deceptive acts or practices engaged in by TRENDnet demonstrates that the FTC has the wherewithal to pursue enforcement actions in today's internet-driven, consumer-focused marketplace.[168]

---

[165] The FTC's complaint detailing the allegations against TRENDnet is available at http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetcmpt.pdf (last visited Mar. 4, 2014).

[166] The settlement agreement between the FTC and TRENDnet is available at http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetorder.pdf (last visited Mar. 4, 2014).

[167] *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy*, FTC, *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles (last visited Mar. 4, 2014).

[168] FTC Commissioner Julie Brill has stated that "if there are data-security or data-use practices that cross the unfairness or deception line, then '[the

Moreover, a sensible assumption could be made that the FTC considers itself as a primary regulator—if not *the* regulator—of consumer privacy concerns.[169] In fact, the FTC's position regarding its enforcement authority over privacy concerns was succinctly laid out in its recent enforcement action against Wyndham Worldwide Corporation ("Wyndham").[170] The FTC brought an enforcement action against the hotel company, as well as its subsidiaries, after it allegedly failed to "maintain reasonable security allow[ing] intruders to obtain unauthorized access to the computer networks of Wyndham Hotels . . . on three separate occasions in less than two years . . . [resulting in] more than $10.6 million in fraud loss."[171] The FTC alleged that Wyndham's failure to secure its customers' data "violated both the deception and unfairness prongs of Section 5(a)" of the FTC Act.[172] Wyndham sought to dismiss the case, contending that "the FTC does not have the authority to bring an unfairness claim

---

FTC] will continue to use [its] law enforcement authority as appropriate.'" McAuley, *supra* note 160.

[169] For example, following Facebook's acquisition of the WhatsApp messaging service, FTC Consumer Protection Bureau director Jessica Rich warned the tech companies that the FTC planned to hold Facebook "to the letter of the law and to its own statements saying that it would not change WhatsApp policies against collecting and sharing personal data with advertisers." Hayley Tsukayama, *FTC warns Facebook, WhatsApp: Keep your privacy promises*, WASH. POST (Apr. 10, 2014), available at http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/10/ftc-warns-facebook-whatsapp-keep-your-privacy-promises.

[170] FTC filings in FTC v. Wyndham Worldwide Corporation, et al. can be found on the FTC's website, available at http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation (last visited Sept. 11, 2014).

[171] F.T.C. v. Wyndham Worldwide Corp., 10 F.Supp.3d 602, 609 (D.N.J. 2014).

[172] *Wyndham Worldwide*, 10 F.Supp.3d at 607.

involving data security," and that "the FTC must formally promulgate regulations before bringing its unfairness claim."[173] The United States District Court for the District of New Jersey ruled on April 7, 2014, that the FTC is at least not precluded from regulating industry data protection standards under Section 5 of the FTC Act.[174] Wyndham has since filed an interlocutory appeal to the United States Court of Appeals for the Third Circuit from the District Court's order; both Wyndham and the FTC have renewed their respective arguments in appellate briefs, and multiple amicus briefs have been filed on behalf of both parties.[175] The District Court's ruling in favor of the FTC, along with the FTC's stated position in the LabMD litigation,[176] certainly gives credence to the FTC's data security *bona fides*.

The FTC should consider CGLI-monitoring device makers to be no different than any other consumer device maker and should take enforcement actions to develop "norms, best practices, and baseline privacy protections" in the CGLI-monitoring industry.[177] By treating CGLI like other sensitive consumer information, device makers could look to past and ongoing FTC enforcement actions for guidance while the FTC

---

[173] *Id.*

[174] The trial court noted that it was in "unchartered territory" but ruled that Wyndham's "demands are inconsistent with governing and persuasive authority." *Id.* at 610.

[175] Briefs from Wyndham and the FTC, as well as amicus briefs from industry and consumer advocacy organizations can be found on the Electronic Privacy Information Center's website covering *FTC v. Wyndham*, available at https://epic.org/amicus/ftc/wyndham (last visited Jan. 12, 2014).

[176] *FTC Affirms Data Security Enforcement Authority in Rejecting LabMD Arguments*, *supra* note 93.

[177] Solove & Hartzog, *supra* note 84.

continues to build upon its privacy "common law of sorts."[178] Enforcement actions would provide a more desirable option for protecting CGLI than relegating consumers to the *status quo* of a lawsuit for breach of contract because of the clear and public signal such action would send to the industry as to what best practices should be followed and what security measures should be developed. Furthermore, FTC guidance through enforcement actions could prove useful in developing precise rules governing CGHI privacy protections. Rather than exist in regulatory limbo waiting for inevitable industry regulation, consumer health device makers could model company policies after enforcement actions against *any* consumer device maker dealing in private consumer information.[179]

This short-term approach would still rely on a case-by-case approach, but CGLI-monitoring device makers would have a larger body of work from the FTC to determine precisely which privacy policies qualify as sufficient consumer protections. CGHI-monitoring devices, however, will require more specific guidance from the FTC.

2. Targeted rulemaking to proactively address privacy concerns in the CGHI-monitoring industry should be developed and adopted

The FTC has enforcement or administrative authority under Section 5 of the FTC Act, as well as over seventy other laws.[180] While these existing laws and enforcement principles

---

[178] *Id.*

[179] *But see,* Manne *supra* note 97.

[180] Statutes are grouped into three categories, including: "(a) Statutes relating to both the competition and consumer protection missions; (b) statutes relating principally to the competition mission; and (c) statutes relating principally to the consumer protection mission." *Statutes Enforced*

can be adapted to new industries and changing markets, a legislative mandate would be more useful to the FTC, device makers, and consumers. Current FTC Chairwoman Edith Ramirez believes the FTC can "fill the void" in consumer data security enforcement left by Congress and has stated that the FTC is seeking "robust security requirements as well as a national breach notice requirement" from Congress to facilitate FTC enforcement actions over data breaches.[181] LabMD's CEO Michael Daugherty recently voiced his displeasure over the current lack of formal data security rules, as well as the aforementioned ruling against his company, stating that he "[does] not mind being law-abiding, [but that he has] to start with knowing what the law is, not some taffy pull of the definition of the word 'reasonable' and 'unfair.'"[182] And consumers as a whole are "interested in understanding how their information is being used," despite a research study commissioned by Microsoft finding that "for the most part people feel they have limited control over how their data is used online."[183]

Direction from Congress is therefore needed to assist the FTC in its enforcement efforts and to help guide future rulemaking as to how CGHI should be protected. Recently-proposed legislation governing consumer data security could

---

or Administered by the Commission, FTC, http://www.ftc.gov/enforcement/statutes (last visited Mar. 4, 2014).

[181] Ben Johnson, *FTC wants stronger rules on consumer data*, MARKETPLACE TECH (Apr. 2, 2014), http://www.marketplace.org/topics/tech/ftc-wants-stronger-rules-consumer-data.

[182] Julian Hattem, *FTC challenger remains defiant over charges*, THE HILL (Apr. 15, 2014, 5:03 PM), http://thehill.com/blogs/hillicon-valley/technology/203611-ftc-challenger-remains-defiant-over-charges.

[183] *Data Privacy Day*, MICROSOFT, http://www.microsoft.com/en-us/twc/privacy/data-privacy-day.aspx (last visited Apr. 16, 2014).

prove helpful to the FTC in this very area. For instance, U.S. Senator John "Jay" Rockefeller, following the Target data breach, introduced the Data Security and Breach Notification Act of 2014.[184] The bill would require the FTC to promulgate regulations governing security practices and notification requirements for a number of entities dealing in personal information.[185] The bill appears to be a necessity based on recent events; however, similar bills have been proposed almost every year for the past decade only to languish in committee.[186]

Critics have opposed data security legislation in the past, declaring it has been too ambiguous to be effective[187] and that companies must already comply with forty-six other state data security laws.[188] Some have argued that the language of some bills actually *reduces* a consumer's ability to sue a

---

[184] S.1976, 113th Congress (2014).
[185] *Id.*
[186] *See, e.g.*, Consumer Data Security and Notification Act of 2005, H.R.3140, 109th Congress (2005); Federal Agency Data Breach Protection Act, H.R.6163, 109th Congress (2006); Notification of Risk to Personal Data Act of 2007, S.239, 110th Congress (2007); Data Breach Notification Act, S.139, 111th Congress (2009); Data Security and Breach Notification Act of 2010, S.3742, 111th Congress (2010); Data Security and Breach Notification Act of 2011, S.1207, 112th Congress (2011); Data Security and Breach Notification Act of 2012, S.3333, 112th Congress (2012); Data Security and Breach Notification Act of 2013, S.1193, 113th Congress (2013).
[187] Paul Kerstein, *Critics Slam Proposed Data Breach Notification Law*, CSO (Nov. 11, 2005, 7:00 AM), http://www.csoonline.com/article/2118922/data-protection/critics-slam-proposed-data-breach-notification-law.html.
[188] James J. Giszczak, *Federal data breach bills pile up in Senate*, MCDONALD HOPKINS (Mar. 18, 2014), http://www.mcdonaldhopkins.com/alerts/data-privacy-and-cybersecurity-federal-data-breach-bills-pile-up-in-senate.

company following a data breach.[189] This uncertainty could be minimized, if not eliminated, by clear guidance from Congress to the FTC on how to proceed in protecting consumer information. Moreover, the number of regulations a device maker would have to comply with could be reduced if state rules are preempted by a federal rule.[190] Device makers, as a result, would benefit from knowing the precise federal regulations by which they must abide and could develop new technologies accordingly.

While the FTC's enforcement actions under its current authority could prove helpful to device makers, comments like those from LabMD's CEO demonstrate the frustrating sense of uncertainty with the *status quo*—a device maker would be constantly unsure if it is properly complying with FTC privacy and security principles. Moreover, enforcement actions come after the fact; and the FTC, consequently, would be only reacting to privacy issues on a case-by-case basis. Importantly for device makers, the rulemaking process would provide a device maker a greater role in policy making, giving it the opportunity to weigh in on the issues it considers important, express its concerns, and share its experiences.

Consumer-generated health information finds itself currently in a middle ground: CGHI is more sensitive than

---

[189] Chris DiMarco, *Data Security Act of 2014 could stitch together patchwork of current regulations*, INSIDE COUNSEL (Jan. 22, 2014), http://www.insidecounsel.com/2014/01/22/data-security-act-of-2014-could-stitch-together-pa.

[190] For example, under the Health Breach Notification Rule, state law is preempted when it conflicts with the federal Rule, but supplements the federal rule when "it is possible to comply with both laws, and the state laws do not thwart the objectives of the federal law." Health Breach Notification Rule, 74 Fed. Reg. 42,965 (Aug. 25, 2009).

most general demographic information but not yet as accurate or detailed as health information gathered by a traditional medical provider. Congress has shown consistency in its unwillingness to pass legislation granting the FTC the express authority to promulgate regulations on data security for a broad range of personal information.[191] At the same time, however, Congress has passed legislation granting the FTC the power to finalize a regulation on notifications for breaches of personal health records.[192] And HHS has shown that rulemaking expanding a federal agency's regulatory purview over companies dealing in health information can be accomplished.[193] The industry is growing in such a way that it will warrant industry-specific requirements. Rather than treat this moment as yet another opportunity to propose fruitless legislation, the regulation of consumer health devices should be used as a test case for even broader consumer protection.[194]

---

[191] *See, e.g.*, Consumer Data Security and Notification Act of 2005, H.R. 3140, 109th Cong. (2005); Federal Agency Data Breach Protection Act, H.R. 6163, 109th Cong. (2006); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Data Breach Notification Act, S. 139, 111th Cong. (2009); Data Security and Breach Notification Act of 2010, S. 3742, 111th Cong. (2010); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Data Security and Breach Notification Act of 2012, S. 3333, 112th Cong. (2012); Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (2013); Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015).

[192] *Health Breach Notification Rule*, *supra* note 90.

[193] *See supra* note 151 (discussing rulemaking expanding HIPAA compliance requirements to Business Associates).

[194] Despite the contention in the FTC's January 2015 Internet of Things staff report that technology-specific legislation is premature, legislation pertaining specifically to consumer health devices should be more likely to find broad enough support in Congress to not languish in committee like previous data breach laws. *See supra* note 159.

The CGHI-monitoring industry is small enough that for the moment, regulatory compliance would be fairly limited in the number of industry players affected. Promisingly, industry best practices, norms, and policies could be developed before poor practices become entrenched in the industry. Words, however, are not enough. Congress should also ensure that the FTC has the proper funding both to cultivate and enforce consumer protection principles in the growing CGHI-monitoring industry.[195]

Finally, consumers will benefit from a specific grant of authority to the FTC to regulate privacy and security issues in CGHI-monitoring devices. Consumers will have a proven industry-regulator to receive complaints, rather than rely on word of mouth or Twitter to voice concerns.[196] Consumers will be able to rely on the threat of civil fines and publicity that comes with an FTC enforcement action—rather than the meager and hard-to-prove damages in a breach of contract claim—to hold device makers accountable. And consumers can rest assured that they will be notified of a breach of their CGHI, thereby affording them the opportunity to quickly minimize the damage from breaches similar to those at Target.[197]

---

[195] McAuley, *supra* note 160.

[196] Consumers are increasingly turning to social media services to publicly resolve customer service issues and complaints. *See, e.g.*, Alan Henry, *How to Get Better Customer Service over Facebook or Twitter*, LIFEHACKER, http://lifehacker.com/how-to-get-better-customer-service-over-facebook-or-twi-1589204317 (last visited Aug. 19, 2014).

[197] Any data security legislation that is signed into law will invariably contain some form of notification requirement. A notification requirement would include quickly informing a consumer of when and how a breach of his CGHI has occurred. A notification requirement could also include

Because of seemingly constant reporting of data breaches in the news, often a consumer's worry over a data breach focuses on the leaking of credit card information, website passwords, or other sensitive financial information.[198] When a consumer's health information has been breached, however, the consequences can be just as grave and at the very least incredibly embarrassing.[199] A consumer's private and sensitive information should be protected. Providing the FTC and consumer health device industry with specific regulations and guidance will ultimately be an advantage, rather than disadvantage, to all parties involved.

V. CONCLUSION

There are different potential solutions to how to protect CGLI and CGHI, but only one solution is acceptable. The market could be allowed to continue its growth while

---

informing a consumer prior to use of his device how the device maker protects its users' CGHI.

[198] *See, e.g.*, John Greenwood, *Heartbleed bug highlights banks' severe cyber security headaches*, FIN. POST (Apr. 12, 2014 , 7:30 AM), http://business.financialpost.com/2014/04/12/heartbleed-bug-highlights-banks-severe-cyber-security-headaches/?__lsa=f361-574a.

[199] M. Eric Johnson, *Data Hemorrhages in the Health-Care Sector, Center for Digital Strategies Tuck School of Business* (2014), *available at* http://digitalstrategies.tuck.dartmouth.edu/cds-uploads/research-projects/pdf/JohnsonEA.pdf ("Data breaches and inadvertent disclosures of customer information have plagued sectors from banking to retail. In many of these cases, lost customer information translates directly into financial losses through fraud and identity theft. The healthcare sector also suffers such data hemorrhages, with multiple consequences. In some cases, the losses have translated to privacy violations and embarrassment. In other cases, criminals exploit the information to commit fraud or medical identity theft.").

consumers rely on corporate promises that consumer-generated lifestyle and health information will be protected. The Department of Health and Human Services could attempt to expand the definition of covered entities under HIPAA to include consumer health device makers. Or the Federal Trade Commission could use its current enforcement authority to prosecute device makers when there is a breach of CGLI while also developing rules to guide the CGHI-monitoring industry going forward.

Ultimately, relying on the FTC is the most desirable option because of the agency's experience with consumer privacy protection in growing technologies. The proper approach, for now, should be to protect consumer-generated lifestyle information the same way that other sensitive consumer information is already protected while also developing regulations for the protection of the more sophisticated consumer-generated health information.