Hastings Communications and Entertainment Law Journal

Volume 38 | Number 1 Article 4

1-1-2015

Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information

Michelle M. Christovich

Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information

by MICHELLE M. CHRISTOVICH*

* J.D Candidate 2015, University of California, Hastings College of the Law. I would like to thank Professor Jill Bronfman for her valuable advice and feedback.

I. Introduction

One of the most prominent recent technological trends has been the rise of personal activity monitors ("fitness trackers")—devices that allow users to track, monitor, and share the minute details of their physical lives. Companies like Fitbit, Jawbone, Apple, Nike, and Garmin offer devices that track a user's heart rate, number of steps taken, activity levels, sleep quality and duration, and calories burned.[1] The various types of sensitive information collected by these devices can be categorized as "personal fitness information" ("PFI"). Additionally, these devices are capable of wirelessly syncing sensitive health information they collect to users' computers, smartphones, and social media accounts.[2]

In the landmark case of *Katz v. United States*,[3] the Supreme Court established that individuals are entitled to a reasonable expectation of privacy.[4] But what constitutes a reasonable expectation of privacy when individuals voluntarily share their private information? The popularity of fitness trackers raises crucial privacy concerns such as how much control users of fitness trackers actually exercise over the use of their PFI and whether that control is meaningful.

This note will address the unique and heightened privacy concerns presented by fitness trackers and address the gaps in current privacy laws, which fail to provide adequate consumer protections or regulation of these devices. Part II of this note will detail the rise in popularity of fitness trackers, the development of privacy rights through case law, and the key

1. *See* Brent Rose, *The Best Fitness Tracker for Every Need*, GIZMODO (Dec. 19, 2014), http://gizmodo.com/the-best-fitness-tracker-for-every-exercise-1673000514.

2. Julia M. Siripurapu, *On the Twelfth Day of Privacy, My True Love Gave to Me . . . 12 Different Types of Wearables!*, NAT'L L. REV. (Dec. 24, 2014), http://www.natlawreview.com/article/twelfth-day-privacy-my-true-love-gave-to-me-12-different-types-wearables.

3. 389 U.S. 347 (1967).

4. *See id.* at 360 (Harlan, J., concurring) (recognizing that "a person has a constitutionally protected reasonable expectation of privacy").

features of the Health Information Portability and Accountability Act of 1996[5] ("HIPAA") in order to provide relevant context to the privacy concerns raised by these devices. Part III will break down the privacy concerns raised by fitness trackers into three separate, but related, categories: (1) The Dangers of the Quantified Self; (2) The Dangers of Using Fitness Trackers in the Employment Context; and (3) The Dangers Associated with Big Data. Each of these categories presents unique privacy concerns and, together, they demonstrate the urgent need for regulating fitness trackers. Accordingly, Part IV proposes a statutory solution modeled after HIPAA, but crafted to explicitly protect the sensitive information gathered and stored by fitness tracking devices. Even though HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), protects against the improper disclosure of private health information,[6] this note contends that the statute does not provide adequate protection to users of fitness trackers because it generally does not apply to those devices. While HIPAA does not typically apply to fitness trackers or PFI, HIPAA is an appropriate statutory model because it outlines a comprehensive approach to protecting sensitive information.

II. Background

A. The Rise of Fitness Trackers

It is no secret that the rise of connected or "smart" devices has been meteoric.[7] According to one study, more than 30 billion devices could be wirelessly connected to the Internet by the year 2020.[8] Fitness trackers, a subset of the Internet of Things, are wearable devices that allow users to track, record, and share every step taken, calorie burned, and hour slept, via the Internet.[9] A study by Pricewaterhouse Coopers indicated that one in five American adults owns a wearable device,[10] and the research firm Canalys reported that eight million activity-tracking bands were expected to ship in 2014.[11] Canalys also estimated that the number of fitness

5. Pub. L. 104-191, 110 Stat. 1936 (104th Cong. 2d Sess., 1996)

6. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/ (last visited Feb. 27, 2014).

7. Brad Turner, *When Big Data Meets Big Brother: Why Courts Should Apply United States v. Jones to Protect People's Data.*, 16 N.C. J.L. & TECH. 377, 392 (2015).

8. *Id.*

9. *See* Siripurapu, *supra* note 2.

10. *Id.*

11. James A. Martin, *Pros and Cons of Using Fitness Trackers for Employee Wellness*, CIO (Mar. 24, 2014), http://www.cio.com/article/2377723/it-strategy/pros-and-cons-of-using-fitness-trackers-for-employee-wellness.html.

trackers expected to ship will rise to 23 million units by 2015 and to more than 45 million by 2017.[12] In fact, seven million fitness bands were sold in Q1 of 2015 alone.[13] While it is difficult to predict the exact number of fitness trackers that will be sold in the next few years,[14] it is clear from this data that fitness tracker sales are rapidly increasing.

As fitness trackers grow in popularity, more companies have introduced their own models.[15] For instance, a December 2014 article published by *Gizmodo* listed nearly 25 different brands that offer, or will soon offer, fitness-tracking devices with features ranging from step counting to sleep tracking and others.[16] For example, Fitbit currently offers six different models of fitness trackers: "Zip," "One," "Flex," "Surge," "Charge," and "Charge HR," which offer a range of features,[17] including steps taken, distance traveled, calories burned, floors climbed, hours slept, alarm functions, heart rate monitoring, GPS tracking, wireless syncing, text notifications, caller ID, music controls, and both online and mobile tools.[18] Similarly, Jawbone currently offers four different models of fitness trackers that include features[19] such as steps and distance tracking, calories burned, food and drink logging, "Smart Coach,"[20] sleep tracking, goal setting, "Smart Alarm," "Idle Alert," heart health monitoring, auto activity classification,[21] water resistance, wireless syncing, a compatible mobile

12. *Id.*

13. Sophie Charara, *If You Own a Fitness Tracker, Chances Are It's a Fitbit*, WAREABLE (May 22, 2015), http://www.wareable.com/fitbit/fitness-tracker-sales-2015-fitbit-1169.

14. Compare estimates presented in Martin, *supra* note 11, to estimates reported in Deborah Lupton, *Self-tracking Modes: Reflexive Self-Monitoring and Data Practices*, NEWS & MEDIA RESEARCH CTR., UNIV. OF CANBERRA (2014), and Zsarlene B. Chua, *Privacy Risks Threaten Future of Wearables*, BUSINESSWORLD (December 23, 2014), http://www.bworldonline.com/content.php?section=Technology&title=privacy-risks-threaten-future-of-wearables&id=100041.

15. *See* Rose, *supra* note 1.

16. *Id.*

17. Some models do not offer all of the features listed. For example, more basic models such as the "Flex" do not include a continuous heart rate monitor, sleep tracking & alarm function, GPS tracking, or floors climbed. *See Find Your Fit*, FITBIT, https://www.fitbit.com/compare (last visited Sept. 15, 2015).

18. *Id.*

19. Some models do not offer all of the features listed. For example, the "UPmove" model does not include the "Smart Alarm," "Idle Alert," heart health monitoring, or auto activity classification features. *See Compare Trackers*, JAWBONE, https://jawbone.com/up/trackers (last visited Sept. 15, 2015).

20. *Id.*

21. *See id.* (stating that this feature, available on all three models, learns habits and recognizes an individual user's activities over time "by using data from the built-in accelerometer and sensors to identify patterns in your movement and automatically associates them with activities").

app, and even the ability to make American Express payments.[22] These are just the features offered by two of the big names behind fitness trackers. This wide range of features demonstrates that consumers are purchasing these devices and using them to track every detail of their physical lives. These devices are, therefore, capable of painting nuanced portraits of their users' health, activity levels, and overall wellness in an unprecedented level of detail.

While these features offer a variety of health benefits,[23] they also raise privacy concerns. Jawbone's auto activity classification and Smart Coach features raise particularly high privacy risks because they use data gathered by the device to identify patterns and make conclusions about a user's activities.[24] The ability of these devices to not only record but also analyze and assess fitness information raises important privacy concerns regarding how this fitness information is transmitted and protected, particularly when companies can share this information with third parties or use it for their own benefit, and even when such information can be used as evidence in a court of law.[25] These are just a few of the privacy concerns raised when individuals voluntarily record and transmit their every move with the help of personal fitness trackers.

B. The Reasonable Expectation of Privacy

In 1890, Samuel Warren and Louis Brandeis first articulated the legal right to privacy.[26] Nearly eighty years later, Justice Harlan set forth the "reasonable expectation of privacy" standard in *Katz*.[27] There, the Court recognized that the Constitution protects what a person seeks to preserve as private, even in a publically accessible area.[28] In *Katz*, the pressing privacy concern was third party surveillance or intrusion upon an individual's

22. *See id.* ("Smart Coach was designed with human nature in mind. It takes all the inputs it receives from your UP® tracker and analyzes that information to give you the personalized advice and insights you need to reach your fitness, sleep and overall health goals.").

23. *See e.g.*, *The Up® System*, JAWBONE, https://jawbone.com/up (last visited Feb. 8, 2015) (inviting users to "[i]mprove the quality of your days and nights through a deeper understanding of how your diet, sleep, activity and the choices you make affect your health and well-being").

24. *See Compare Trackers*, JAWBONE, *supra* note 19.

25. *See* George Waggott & Wilson McCutchan, *Fitbit Evidence: Coming Soon to a Court Near You*, MONDAQ (Nov. 21, 2014), http://www.mondaq.com/canada/x/355492/employment+litigation+tribunals/Fitbit+Evidence+Coming+Soon+To+A+Court+Near+You (reporting that a Canadian litigator will rely on Fitbit tracking information as evidence that his client suffered debilitating personal injuries).

26. Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (Dec. 1890) (recognizing the "right to be let alone").

27. *See* Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring) (". . . [A] person has a constitutionally protected reasonable expectation of privacy.").

28. *Id.* at 351.

privacy, typically when the individual is unaware that they are being recorded.[29] While the "reasonable expectation" standard of privacy may have been appropriate in the late 1960s, it is unclear how that standard translates into the modern technological realities of fitness trackers, Facebook, and Twitter when individuals routinely record and share the details of their daily lives. Today, the concerns around privacy have shifted dramatically because contemporary surveillance is no longer just third party surveillance, but also "self-surveillance."[30] Scholars have described the phenomenon of self-surveillance as "[u]sing various existing and emerging technologies, such as GPS-enabled smartphones, we are beginning to measure ourselves in granular detail—how long we sleep, where we go, what we breathe, what we eat, how we spend our time."[31]

Thus, the fundamental difference between the surveillance contemplated in *Katz* and self-surveillance is that, for self-surveillance, "the threat may actually come from *ourselves*."[32] According to one scholar, "[n]early everything people do today becomes data. And nearly every bit of data is shared, knowingly or unknowingly, voluntarily or involuntarily, with others."[33] Moreover, much of this data is collected, as in the case of fitness trackers, because individuals are voluntarily and intentionally participating in self-surveillance. What limits can the reasonable expectancy of privacy standard provide when individuals are intentionally recording their thoughts, activities, and behaviors and sharing them with the world?[34] In other words, how does the reasonable expectation of privacy function when consumers voluntarily share their fitness information to a select group of people or even publicly?

Although the Third Party doctrine has established that anything a person knowingly exposes to the public is in the public sphere and, therefore, not subject to the Fourth Amendment, that doctrine has been called into question.[35] Notably, in *United States v. Jones*, Justice Sotomayor's concurrence challenged the Third Party doctrine, calling it "ill

29. *Id.*; *See also* Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke, and Mark Hansen, *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 825 (2012) ("In the standard privacy problem, personal data are collected by some counterparty in the course of an individual's interaction with that counterparty.").

30. Kang et al., *supra* note 29, at 814.

31. *Id.* at 812.

32. *Id.*

33. *See* Turner, *supra* note 7, at 381.

34. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (recognizing that the reasonable expectation of privacy has changed in the digital age, in which people regularly reveal a great deal of information about themselves to third parties).

35. *See* Katz v. United States, 389 U.S. 347, 351 (1967); United States v. Miller, 425 U.S. 435, 442 (1976), *superseded by statute*, Right to Financial Privacy Act, 12 U.S.C.S. §§ 3401–3422, *as recognized in* Dadidov v. SEC, 415 F. Supp. 2d 386, 387 (S.D.N.Y 2006).

suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[36] She stated that she "would not assume that all information voluntarily disclosed . . . for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[37] This note contends, as Justice Sotomayor suggests, that users do not forfeit their reasonable expectation of privacy simply because they have shared fitness information with companies like Fitbit and Jawbone for limited health-related purposes. While user expectations may be somewhat limited, they can still reasonably expect that their information will only be used as outlined in company privacy policies[38] for specific purposes and should still retain control over how their information is shared with third parties. For example, if a company shares user information in violation of its own privacy policy, the Federal Trade Commission can impose fines under the Federal Trade Commission Act ("FTCA").[39] Thus, the reasonable expectation of privacy standard still applies in the digital age and is strengthened by statutes like the FTCA and HIPAA, which protect against the improper uses of personal information.

C. The Health Information Portability and Accountability Act of 1996

HIPAA was enacted in 1996 and amended by the HITECH ("the Act") in 2009.[40] The Act protects against the improper disclosure of individually identifiable health information held by covered entities and their business associates.[41] The purpose behind the Act is to balance protecting individuals' health information with permitting the disclosure of health information necessary for effective patient care.[42] HIPAA achieves this purpose by establishing the first set of national standards for protecting health information.[43] However, HIPAA is limited because it does not apply to all health information or all companies that handle health information.[44]

36. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

37. *Id.*

38. *See infra* Section III.

39. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 134 (2013).

40. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 6.

41. *Health Information Privacy*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html (last visited Feb. 27, 2014).

42. *Id.*

43. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 6.

44. *See id.*

HIPAA only covers Protected Health Information ("PHI"),[45] which is defined as "individually identifiable health information."[46] In addition, HIPAA only applies to covered entities—health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form—and their business associates.[47]

Although HIPAA does not cover fitness trackers or PFI, its comprehensive approach to protecting sensitive information serves as a strong model for protecting PFI. HIPAA provides substantial protections by requiring Notice, Right of Access, and Authorization.[48] While the Notice requirement establishes that covered entities must give notice regarding their privacy practices, the Right of Access requirement grants patients the right to access any PHI used to make decisions about them.[49] Additionally, the Authorization requirement establishes that patient authorization is required for all uses and disclosures of health information, except for treatment, payment, or healthcare operations.[50] HIPAA also explicitly requires patient authorization in order to use data for marketing purposes.[51]

HIPAA consists of three primary parts: (1) *The Standards for Privacy of Individually Identifiable Health Information* ("The Privacy Rule"),[52] (2) *The Security Standards for the Protection of Electronic Protected Health Information* ("The Security Rule"),[53] and (3) The HITECH Act.[54] The Privacy Rule aims to limit the circumstances in which PHI may be used or disclosed.[55] It provides that "[a] covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request."[56]

45. *Id.*

46. *See* SOLOVE & SCHWARTZ, *supra* note 39, at 134.

47. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 6.

48. SOLOVE & SCHWARTZ, *supra* note 39, at 104.

49. *Id.*

50. *Id.*

51. *Id.*

52. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 6.

53. *Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html (last visited Feb. 27, 2014).

54. *HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html (last visited Feb. 27, 2014).

55. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 6.

56. *Id.*

Unlike the Privacy Rule, the Security Rule only applies to electronic protected health information ("e-PHI"), a subset of PHI that includes "all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form."[57] The Security Rule establishes standards for protecting e-PHI by requiring technical and non-technical safeguards.[58] These safeguards include training and hiring security personnel, workforce training, ensuring facility access and control, workspace and device security, controlling access, and ensuring protected information is not improperly altered or deleted.[59] While the Security Rule takes a flexible, case-by-case approach to protecting e-PHI, it establishes four basic requirements of covered entities: (1) ensuring the confidentiality and integrity of e-PHI they create or transmit; (2) identifying and protecting against threats to security; (3) protecting against reasonably anticipated impermissible uses or disclosures; and (4) ensuring compliance by its workforce.[60]

The HITECH Act, enacted in February 2009,[61] establishes notification requirements for data security breaches of covered entities that involve PHI.[62] The Act defines a breach as "an unauthorized disclosure of unencrypted PHI."[63] Additionally, it establishes that notification must be given "without reasonable delay,"[64] requires that breaches that affect more than 500 individuals must be reported to the media,[65] and extends HIPAA to cover business associates.[66] Together, these three components of HIPAA provide the foundation for a comprehensive approach to protecting PHI held by covered entities and business associates.

Adopting a similar approach to data collected by fitness trackers would provide comprehensive protection of PFI. Protections like the Security Rule and the data breach notification requirements of the HITECH Act are especially important in the context of fitness trackers because PFI is almost exclusively electronic information, which presents particularly high security and data breach risks.

57. *HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 54.

58. *Id.*

59. *Id.*

60. *Id.*

61. *Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 53..

62. SOLOVE & SCHWARTZ, *supra* note 39, at 99, 107.

63. *Id.* at 107

64. *Id.*

65. *Id.*

66. *Id.* at 103.

HIPAA does not provide a private right of action.[67] Instead, the Department of Justice is responsible for criminal enforcement, while the Department of Health and Human Services ("HHS") is responsible for civil enforcement through its Office of Civil Rights.[68] However, scholars such as Daniel Solove and Peter Winn have pointed out that plaintiffs have been able to use HIPAA to establish standard of care when bringing common law actions under state law.[69] Solove explains, "[f]or breach of confidentiality, courts look to norms, ethical rules, and laws to determine the duties that caregivers owe to patients. HIPAA is a law that establishes duties, and thus serves as a useful source of duties for the common law."[70] For example, as Solove observes,[71] both the Connecticut Supreme Court in *Byrne v. Avery Center for Obstetrics and Gynecology*[72] and the West Virginia Supreme Court[73] held that HIPAA may be used to establish the standard of care in negligence claims. Winn also argues, "the HIPAA Privacy Rules are likely to be adopted in private state actions for breach of confidentiality as establishing the duty."[74] Thus, HIPAA not only establishes a comprehensive approach to protecting sensitive health information enforced by federal agencies, but also aids plaintiffs seeking to bring common law claims for invasions of privacy. Applying Solove and Winn's work to the fitness tracker context, the HIPAA model demonstrates that a private right of action may not be necessary in order to effectively protect PFI.

III. The Heightened Privacy Concerns Presented By Using Fitness Trackers to Record and Transmit Personal Fitness Information

A. The Dangers of the Quantified Self

The natural product of self-surveillance is the "Quantified Self." The Quantified Self Movement takes advantage of technology in order to

67. *Id.* at 99.

68. *Id.* at 106.

69. *See* Daniel Solove, *Lawsuits for HIPAA Violations and Beyond: A Journey Down the Rabbit Hole*, LINKEDIN PULSE (Nov. 8, 2014), https://www.linkedin.com/pulse/20141118051323-2259773-lawsuits-for-hipaa-violations-and-beyond-a-journey-down-the-rabbit-hole?trk=mp-reader-card; Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 619–20 (2002).

70. Solove, *supra* note 69; Winn, *supra* note 69, at 619–20.

71. Solove, *supra* note 69.

72. Byrne v. Avery Ctr. for Obstetrics and Gynecology, No. 18904, 2014 WL 5507439 (Conn. Nov. 11, 2014)

73. R.K. v. St. Mary's Med. Ctr., 735 S.E.2d 715 (W.Va. 2012).

74. Winn, *supra* note 69, at 19–20.

encourage self-awareness by tracking data relating to an individual's exercise, diet, sleep habits, health maintenance, financial management, learning, and general wellness.[75] Although fitness trackers may provide significant benefits in terms of health and wellness, the level of detail that these devices can convey about their wearers' private lives raises unique and heightened privacy concerns.[76] Wearable devices like fitness trackers present especially high privacy risks "because of the kinds and volume of data they collect. This includes, but isn't limited to, email addresses, logins, passwords and other credentials; steps; heart-rate information; physical addresses, routes travelled and other location data; sleep habits, and height and weight details."[77] In the words of Kevin Haley, the Director of Symantec's Security Response Team, "[i]t's the nature of the data that's being collected . . . . This is really getting to the essence of our being. It's hard to believe people are willing to share all this stuff, especially around health."[78]

Arguably, a greater cause for concern is not simply the volume and type of data being collected, but what the data is used for and where it is sent. For example, a recent test of twelve fitness apps performed by the Federal Trade Commission ("FTC") found that those apps transmitted personal information and other data to 76 different entities.[79] What is more alarming is that an FTC Commissioner admitted, "[w]e don't know where that information ultimately goes."[80]

When it comes to the Quantified Self, it is difficult to imagine that consumers can make meaningful or informed decisions about privacy and the collection of massive amounts of sensitive health information when they are unaware of who receives that information or the reason it is being collected. As Haley points out, "[i]n five years, we'll discover it's being used in ways we couldn't have guessed. In the short term, people may not care if people know how much they weigh, but . . . we may not ultimately want people to have that information."[81]

75. Turner, *supra* note 7, at 388 (citing Joseph Bradley, *When IoE Gets Personal: The Quantified Self Movement!*, CISCO BLOG (Sept. 10, 2013), http://blogs.cisco.com/zzfeatured/when-ioe-gets-personal-the-quantified-self-movement/).

76. *See* Al Sacco, *Fitness Trackers Are Changing Online Privacy—and It's Time to Pay Attention*, TECH HIVE (Aug. 15, 2014), http://www.techhive.com/article/2465820/fitness-trackers-are-changing-online-privacy-and-its-time-to-pay-attention.html.

77. *Id.*

78. *Id.*

79. Editorial, *Smart Watches and Weak Privacy Rules*, N.Y. TIMES (Sept. 15, 2014), http://www.nytimes.com/2014/09/16/opinion/smartwatches-and-weak-privacy-rules.html?_r=0.

80. *Id.*

81. *See* Sacco, *supra* note 76.

Another concern, which is often overlooked, is the different levels of sharing. A user may be comfortable sharing her PFI with a select group, for example, all of her friends or her workout group. However, simply because that user has chosen to share her PFI with a particular group does not mean that she has given permission for her information to be shared with advertisers or the general public. Additionally, the fact that a user has shared PFI for one purpose, such as assisting in reaching fitness goals, does not mean she should be required to share that information for other purposes like advertising. The fact that users have chosen to share certain information does not necessarily indicate they have completely forfeited any reasonable expectation of privacy in that information. In fact, the choices individuals make about who to share their PFI with, when to share, and what that information may be used for, strongly suggest that users expect their fitness information to only be shared in particular ways and for particular purposes dictated by the users' choices.

B. Fitbit in the Office: Incentivized Sharing of Fitness Information in the Employment Context

Fitness trackers raise particularly high concerns because they present new types of privacy problems. Unlike the traditional privacy concerns of third-party surveillance,[82] users of fitness trackers *voluntarily* record and transmit their lives in granular detail. Thus, the most pressing issue is not whether users are being recorded, but what happens to the sensitive information collected by fitness trackers after users have intentionally and voluntarily shared it.

Concerns over how PFI is used are particularly poignant when fitness trackers are used in the employment context. Many employers are beginning to incorporate fitness trackers into wellness programs as a tool for improving their employees' health.[83] The research firm Gartner estimates that 10,000 companies offered fitness trackers to their staff in 2014.[84] Fitbit, for example, has begun selling its devices to employers

82. Kang et al., *supra* note 29, at 825 ("In the standard privacy problem, personal data are collected by some counterparty in the course of an individual's interaction with that counterparty.").

83. *See* Lisa Evans, *Is the Quantified Employee a Healthier Employee?*, FAST CO. (Sept. 2014), http://www.fastcompany.com/3036364/wearables-week/is-the-quantified-employee-a-healthier-employee ("According to ABI Research, more than 13 million wearable fitness tracking devices are expected to be incorporated into employee wellness programs within the next five years."); *see also* Martin, *supra* note 7 ("By 2018, more than 13 million wearable activity-tracking devices will be integrated into employee wellness programs, based on estimates from ABI research.").

84. Stuart Dredge, *Why the Workplace of 2016 Could Echo Orwell's 1984*, THE GUARDIAN (Aug. 22, 2015), http://www.theguardian.com/technology/2015/aug/23/data-and-tracking-devices-in-the-workplace-amazon.

who, with their employees' permission, "can then track their workers' health, see how active individual employees are, and foster a little healthy competition."[85] Both employers and employees seem to benefit from this exchange,[86] but the trend also seems to be incentive-based: employees agree to wear fitness trackers and, in exchange, receive benefits from their employers.[87] For instance, Shannon Daly, Vice President of Human Resources at the cloud-consultancy firm Apriro, suggests that companies "[o]ffer the fitness trackers as an incentive and give them away where possible . . . . Provide challenges that motivate employees to participate in your company wellness program using the tracker. Be transparent and explain how the employee metadata results may be used."[88]

Another example of this incentive-based approach is Bates College, which recently offered Fitbit "Zip" devices to employees in order to encourage participation in its employee wellness competition (called "Ready, Set, Go").[89] Thirty-five percent of the college's 700 employees currently participate in the program.[90] According to the program's director, Mike Milliken, "[w]hen we issued them initially, we were upfront about the fact it wasn't simply a gift for signing up. . . . They needed to *earn* it by using it, and that seems to be driving engagement."[91] Even though employees voluntarily participate in these programs, using fitness trackers in employee wellness programs still raises significant privacy concerns as to whether employers are using the information gathered by such devices appropriately.[92] In fact, journalist Jack Smith has anticipated the dangers that will likely arise when employers receive their employees' private health information: ". . . once premiums and plans are directly tied to employees' day to day health, it's pretty easy to imagine a world where company culture, or even hiring decisions, are driven by individual

85. Jack Smith IV, *Fitbit Is Now Officially Profiting From Users' Health Data*, OBSERVER (Apr. 18, 2014), http://observer.com/2014/04/fitbit-is-now-officially-profiting-from-users-health-data/#ixzz2zdt0LO2w; *see also* Martin, *supra* note 11 ("Fitness trackers, mobile apps and Web-based dashboards let workers count calories and steps, monitor sleep patterns, compete against colleagues and earn prizes.").

86. *See* Evans, *supra* note 83.

87. Martin, *supra* note 11.

88. *Id.*

89. *Id.*

90. *Id.*

91. *Id.* (quoting Mike Milliken) (emphasis added).

92. *See* John F. Wasik, *Employers' Health Care Push: Play by Our Rules, or Pay*, THE FISCAL TIMES (Mar. 6, 2014), http://www.thefiscaltimes.com/Columns/2014/03/06/Employers-Make-Health-Care-Push-Play-Our-Rules-or-Pay#sthash.IAjxaAi8.dpuf ("[E]mployers are increasingly calling the shots on how employees receive their benefits—and workers may be penalized or rewarded depending upon how they take care of themselves. That means they may be subject to regular monitoring and told to enroll in health care management programs.").

fitness."[93] For example, suppose two employees are up for the same promotion, and Employee A volunteers to wear a fitness tracker provided by the employer, but Employee B does not. Could the employer assume Employee B is less of a team player than Employee A and hold that assumption against him?

This example demonstrates another danger: whether an employee's choice to participate in a fitness-tracker-based wellness program will remain truly voluntary. In his article, "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future," Scott Peppet argues that companies are able to extract private information that they ordinarily could not obtain by offering economic incentives to consumers who share that information.[94] The real danger, however, occurs when such incentive-based exchanges of sensitive, personal information become the norm: "[a]lthough at first consumers may receive a discount for using a driving or health monitor, privacy may unravel as those who refuse to disclose are assumed to be withholding negative information and therefore stigmatized and penalized."[95] It is easy to imagine how this concern could translate into a workplace environment. Once a critical mass of employees begins voluntarily exchanging private health information for incentives through fitness trackers, it is probable that employers will assume that those who refuse to do so have something to hide. While it is easy to imagine the negative consequences that might result from such assumptions—denial of opportunities, promotions, etc.—those who are affected are unlikely to receive redress for these injuries because instances of negative discrimination are difficult to prove. Because of the danger that PFI will be used for discriminatory purposes, fitness tracker regulation is necessary to prevent the use of PFI for discriminatory or other improper purposes.

C. Big Data Is Always Watching: The Dangers of Big Data and Fitness Trackers

Fitness trackers have the potential to cause especially egregious invasions of privacy when the health information gathered by such devices ends up in the hands of Big Data. Big Data can be defined as a "problem-solving philosophy that leverages massive datasets and algorithmic analysis to extract 'hidden information and surprising correlations.'"[96] Unlike the surveillance at issue in *Katz*, which was collected for a specific purpose and

93. Smith, *supra* note 85.

94. Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U.L. REV. 1153, 1155 (2011).

95. *Id.* at 1156.

96. Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81 (Sept. 2013).

likely kept for a limited period of time,[97] the data collected by fitness trackers can be retained indefinitely on a company's servers. This section will demonstrate that the combination of fitness trackers and Big Data is particularly threatening to privacy rights for three primary reasons: (1) there is a lack of awareness about the use of information by Big Data that prevents users from making informed decisions about sharing their private information; (2) even if consumers do understand the impact of Big Data, data gathered today will likely have unexpected future uses; and (3) the line between de-identified and identifying data is becoming increasingly blurry because it is becoming easier to identify users through information that both users and companies treat as anonymous. While each of these issues presents privacy concerns on its own, together these three problems seriously undermine the ability of current protections to adequately secure individual privacy rights by breaking down privacy protections from three different, but related, directions.

1. Consumers' Lack of Perception About the Predictive Power of Big Data Compromises Their Ability to Make Informed Decisions About Their Fitness Information

One of the most basic dangers presented by fitness trackers is the lack of consumer awareness about how PFI can be used when it is collected in the aggregate. Turner provides the example of the two-way mirror to illustrate this problem: "the end-user sees her own activities reflected in the two-way mirror, and does not realize that on the other side, she is actually being observed by any number of faceless, non-descript organizations that she probably does not even know exist."[98] Because consumers are not fully cognizant of how their information will be used once it is collected by fitness trackers, it is difficult for users to make informed choices about how, when, or even if they should record and share the nuances of their daily lives. In fact, many of the privacy protections currently relied upon, such as Privacy Policies, Terms of Service, and "Opt-In" policies, require consumers to be informed in order to be effective. Put simply, consent is less probative when users do not fully understand what they are consenting to. Without effective understanding of how data will be used when collected in the aggregate, users are susceptible to "sleepwalking into a surveillance society."[99]

In a recent paper, researchers from Clemson University conducted qualitative content analysis of online comments related to users' privacy

97. *See* Katz v. United States, 389 U.S. 347 (1967).

98. *See* Turner, *supra* note 7, at 383.

99. Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. 25 (2013).

concerns about wearable devices.[100] They found that users perceived devices worn on the wrist, including fitness trackers, as presenting fewer privacy concerns than other devices.[101] The researchers suggest that users likely do not understand how this data can be misused by third parties, the privacy implications that arise when data is retained for long periods of time, or how this data can be combined with complementary data.[102] For instance, despite finding that users do not perceive devices like fitness trackers as threatening, the authors' analysis suggests that GPS sensors present the most critical privacy concerns for users of wearable devices.[103] Thus, this research suggests that users have a false sense of security when it comes to fitness trackers—they mistakenly view these devices as having fewer privacy concerns even though activity trackers involve critical privacy concerns like tracking and recording user locations.

This lack of awareness seems to stem from users' perception of fitness trackers as harmless, innocuous devices. Australian privacy advocate and researcher Katina Michael has addressed consumers' misconceptions about fitness trackers by going so as far as to compare fitness trackers to "state surveillance anklets."[104] She declared, "[w]e're being duped into thinking they're liberating devices, when they're devices of enslavement. . . . And consumers aren't saying 'uh-oh, there's a problem here'. *They're saying 'bring it on*!'"[105] While Michael's comments may seem harsh, her point is critical: consumers often underestimate and place too much trust in their fitness trackers.

One explanation for users' false sense of security regarding fitness trackers is the fact that these devices are often worn like fashion accessories or jewelry[106] and, consequently, blend seamlessly into users' daily lives. For example, Leaf, a new fitness tracker set to hit the market in May 2015, is designed to be worn as a necklace and is even marketed as

100. Vivian Genaro Motti & Kelly Caine, *Users' Privacy Concerns About Wearables: Impact of Form Factor, Sensors and Type of Data Collected* 1 CLEMSON UNIV., http://fc15.ifca.ai/preproceedings/wearable/paper_2.pdf.

101. *Id.* at 4.

102. *Id.* at 5.

103. *Id.* at 4.1.

104. Richard Chirgwin, *Welcome to 'Uber-veillance' Says Australian Privacy Foundation*, THE REGISTER (Jan. 13, 2015), http://www.theregister.co.uk/2015/01/13/its_already_too_late_for_privacy/.

105. *Id.*

106. *See* Molly Wood, *Jawbone Up3 Band Takes Tracking to the Extreme*, N.Y. TIMES (Nov. 6, 2014), http://bits.blogs.nytimes.com/2014/11/06/jawbone-up3-band-takes-tracking-to-the-extreme/?ref=technology&_r=0. (describing how Jawbone's fitness tracking devices increasingly look like jewelry and reporting that Jawbone encourages its partners to design versions that look even more like bracelets than activity monitors).

"the world's smartest piece of jewelry."[107] Apple and Fitbit both offer interchangeable bands designed by luxury brands such as Hermès and Tory Burch,[108] and the newly released Apple Watch is advertised as not only a powerful, multifaceted smart device, but also a "true expression of your personal taste."[109] Because fitness trackers are deigned to blend into users' lifestyles, users are unlikely to seriously consider the privacy implications raised by such devices and are more likely to view them as innocuous everyday objects. This misperception of fitness trackers poses serious threats to protecting user privacy. While users may understand the privacy risks associated with wearing fitness trackers, they are less likely to view these concerns seriously if they think of their fitness tracker as a stylish, harmless accessory. The tendency to underestimate these privacy concerns will, therefore, undermine privacy protections such as requiring Privacy Policies, agreeing to Terms of Service, and "Opt-In" approaches by diminishing the level of care users exercise when deciding whether to opt in or agree to a company's policies.[110]

2. Because Data Gathered Today Will Likely Be Used for Unforeseen Purposes, It Is Unlikely that Current Privacy Protections Will Be Able to Adequately Guard Against Future Uses of Data

Even assuming that users do fully appreciate the privacy concerns surrounding the *current* uses of data gathered by fitness trackers, sensitive information gathered and shared by connected devices is often used for unforeseen purposes. While users may make informed decisions about casually sharing personal information in one context, it is becoming much easier for seemingly innocuous data to be used to elicit unexpectedly revealing information.[111] For example, a recent study suggests that a computer model can predict individual personality traits such as how much someone drinks, whether they do drugs, and what subject they are likely to

107. *See* BELLABEAT, https://www.bellabeat.com (last visited May 5, 2015) (describing the Leaf fitness tracker with the tagline "technology meets fashion").

108. *See Hermès*, APPLE, http://www.apple.com/apple-watch-hermes/ (last visited Sept. 15, 2015); *see also Tory Burch for Fitbit*, FITBIT, https://www.fitbit.com/toryburch (last visited Sept. 15, 2015).

109. *Apple Watch*, APPLE, http://www.apple.com/watch/?cid=wwa-us-kwg-watch-com (last visited May 5, 2015).

110. *See e.g.*, Emma Hutchings, *Fitbit Users' Sexual Activity Found In Google Search Results*, PSFK (July 4, 2011), http://www.psfk.com/2011/07/fitbit-users-sexual-activity-found-in-google-search-results.html (reporting that users who were not careful with their privacy settings inadvertently allowed their sexual activity data, collected and shared by FitBit, to appear in Google search results).

111. *See* Anna North, *How Your Facebook Likes Could Cost You a Job*, N.Y. TIMES (Jan. 20, 2015), http://op-talk.blogs.nytimes.com/2015/01/20/how-your-facebook-likes-could-cost-you-a-job/?_r=1.

study, based solely on that person's Facebook likes.[112] Other researchers assert that Facebook likes can reveal attributes, including gender, sexual orientation, race, intelligence, and political leanings.[113] While Facebook likes, like fitness trackers, are seemingly harmless, these studies demonstrate that the door is open for automated psychological assessment and other inferences based on an individual's digital footprint and performed without permission or notice.[114] Similarly, in a recent FTC Staff Report, one researcher hypothesized that "although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user's suitability for credit or employment."[115] For instance, researchers at the University of Illinois have developed an app for smart watches that can track the keystrokes made by someone wearing the device.[116] While the app is still in its early stages and has not yet been perfected, the researchers anticipate that this technology could result in "motion leaks" and could potentially reveal personal information like passwords and login credentials.[117] As one user attempts to use Fitbit as evidence in a Canadian personal injury case,[118] this raises further questions about how the health information gathered by fitness trackers could have

112. *Id.*

113. *See* Adi Kamdar & Dave Maass, *You Won't Like What Your Facebook 'Likes' Reveal*, ELEC. FRONTIER FOUND. (Mar. 13, 2013), https://www.eff.org/deeplinks/2013/03/facebook-likes-reveal-sensitive-personal-information (reporting that researchers, based on Facebook likes, were able to predict whether a user was African American or white 95% of the time, male or female 93% of the time, sexual orientation 88% of the time for men and 75% of the time for women, political leaning (Republican versus Democrat) 85% of the time, and whether your parents divorced when you were a kid 60% of the time, make reasonably accurate guesses about whether you were a drug user, drinker, or smoker, as well as a host of other attributes, including emotional stability, satisfaction with life, and extraversion).

114. *See id.* (stating that information individuals share for one purpose can now easily be collated and acted upon "for wildly different purposes"); *see also* North, *supra* note 111.

115. FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, FTC STAFF REPORT (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

116. Victoria Woollaston, *Smartwatch Hack Lets Criminals Know What You're TYPING: Motion Sensors Can Remotely Reveal Which Keys You're Pressing*, DAILY MAIL (Sept. 11, 2015), http://www.dailymail.co.uk/sciencetech/article-3230815/Smartwatch-hack-lets-criminals-know-TYPING-Motion-sensors-remotely-reveal-keys-pressing.html.

117. *Id.*

118. *See* Kate Crawford, *When Fitbit Data Is the Expert Witness*, THE ATLANTIC (Nov. 19, 2014), http://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/.

unanticipated significance in future legal cases, employment decisions, disability claims, or insurance benefits.[119]

The concerns surrounding unanticipated uses of PFI are both distinct from and related to the underestimation of the privacy risks associated with these devices. While both issues deal with users' difficulty or resistance to grasping the privacy risks that currently exist, the unforeseen future uses of private information raise particularly high privacy concerns because this problem might not be solved by simply providing notice or educating consumers about the risks of sharing data. Even someone who makes careful and considered decisions about sharing information cannot be certain that their data will not be used for some unanticipated and detrimental purpose in the future.

3. As It Becomes Easier to Re-identify Users Through "Anonymized" Data, the Line Between Identifying and Non-identifying Data Is Beginning to Disappear

The ability of users to effectively control how their own fitness data is used and shared is further complicated by the blurring line between identifying and non-identifying data.[120] Most companies that offer fitness tracking devices draw a distinction between sharing non-identifying and identifying data with third parties.[121] Fitbit's privacy policy, for example, permits the company to share and sell aggregated, de-identified data for research or reports about health and fitness.[122] For example, shortly after

119. *See id.* ("The current lawsuit is an example of Fitbit data being used to support a plaintiff in an injury case, but wearables data could just as easily be used by insurers to deny disability claims, or by prosecutors seeking a rich source of self-incriminating evidence.").

120. *See* Giulio Coraggio, *What is Anonymous Data?*, GAMING TECH L.BLOG (May 12, 2014), http://www.gamingtechlaw.com/2014/05/what-is-anonymous-data.html ("Problems relating to what data/images/information can be consider [sic] anonymous is one of the major data protection issues of privacy law having an impact in any sector including the Internet of Things, eHealth and on any activity that tries to rely on Big Data or in general large databases.").

121. *See e.g.*, *Fitbit Privacy Policy*, FITBIT, http://www.fitbit.com/privacy (last visited Feb. 10, 2015) ("First and foremost: We don't sell any data that could identify you. We only share data about you when it is necessary to provide the Fitbit Service, when the data is de-identified and aggregated, or when you direct us to share it."); *Website Privacy*, JAWBONE, https://jawbone.com/privacy (last visited Feb. 10, 2015) ("We do not rent, sell or otherwise share your individual, personal information with third parties . . . We share aggregated usage statistics that cannot be used to identify you individually."); *Basis Privacy Policy*, BASIS, https://www.mybasis.com/legal/privacy/ (last visited Feb 10, 2015) ("We may share or sell aggregated, de-identified data with third parties, including, but not limited to, for marketing purposes or with research organizations"); *Privacy Policy*, WITHINGS, http://www-media-cdn.withings.com/wysiwyg/legal/2015-Privacy-policy-VUS.pdf?_ga=1.84430169.1929328589.1423651096 (last visited Feb. 10, 2015) ("We undertake not to sell your personal data without your prior agreement. At Withings, we firmly believe that data can serve the collective interest. We may produce statistics and analyses using collected data. They would first be anonymized and aggregated beforehand to assure your privacy to be protected.").

122. FitBit *Privacy Policy*, *supra* note 121.

the 2015 Super Bowl, Fitbit used fitness information gathered by its devices to measure and track its users' excitement throughout the game by examining users' heart rates.[123] Fitbit's Privacy Policy explains, "[w]hen we provide this information, we perform appropriate procedures so that the data does not identify you and we contractually prohibit recipients of the data from re-identifying it back to you."[124] Thus, the line between identifying and non-identifying data is critical because many companies and privacy regulations[125] use that line as the boundary for determining which data may be shared with, or even sold to, third parties. As that line blurs (because it is becoming easier to reidentify anonymized data[126]), many of the privacy safeguards currently in place will become ineffective and relatively meaningless, leaving consumers vulnerable to potentially vast invasions of privacy, ranging from unforeseen uses of data to the re-identification of supposedly anonymous data.

Recently, researchers have been calling attention to the ease with which de-identified information can be reidentified, exposing users' identities, by cross-referencing that data with other data sets.[127] As early as 2000, researcher Latanya Sweeney showed that eighty-seven percent of Americans could be identified using only their birth date, zip code, and sex.[128] After Netflix released an anonymized data set of 100 million movie ratings collected from nearly half a million users as part of a contest in 2006, researchers Arvind Narayanan and Vitalu Shmatikov were able to "unmask" these anonymous users by cross-referencing the anonymized data, which included timestamps, with non-anonymized movie ratings

123. Robert DS, *Heart-Racing Moments from the Big Game*, THE FITBIT BLOG (Feb. 3, 2015), http://blog.fitbit.com/heart-racing-moments-from-the-big-game/#i.ml8qpjotef9hur.

124. *Id.*

125. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010) ("[N]early every information privacy law or regulation grants a get-out-of-jail-free cardto those who anonymize their data.").

126. *See e.g.*, Nate Anderson, *"Anonymized" Data Really Isn't—and Here's Why Not*, ARS TECHNICA (Sept. 8, 2009), http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/; Kim Zetter, *The World's Most Wired Computer Scientist: Arvind Narayanan*, WIRED (June 18, 2012), http://www.wired.com/2012/06/wmw-arvind-narayanan/; Nate Anderson, *Pulling Back the Curtain on "Anonymous" Twitterers*, ARS TECHNICA (Mar. 31, 2009), http://arstechnica.com/tech-policy/2009/03/pulling-back-the-curtain-on-anonymous-twitterers/.

127. *See* Ohm, *supra* note 125, at 716 (arguing that researchers have essentially "blown up" the robust anonymization assumption, casting doubt on the ability of de-identification to adequately protect users' identities); Anderson, *"Anonymized" Data Really Isn't—and Here's Why Not*, *supra* note 126; Anderson, *Pulling Back the Curtain on "Anonymous" Twitterers*, *supra* note 126; Eric Bangeman, *AOL Subscribers Sue Over Data Leak*, ARS TECHNICA (Sept. 26, 2006), http://arstechnica.com/business/2006/09/7835/; Zetter, *supra* note 126.

128. Anderson, *"Anonymized" Data Really Isn't—and Here's Why Not*, *supra* note 126.

posted publicly on the Internet Movie Database.[129] In 2009, Narayanan and Shmatikov used similar methods on Twitter and Flickr to demonstrate once again that data can easily be cross-referenced with other data sets in order to expose users' identities.[130] In that case, they found that one-third of users who have accounts on both Twitter and Flickr could be identified on Twitter using their Flickr connections.[131] Like Netflix, AOL also inadvertently exposed users to privacy intrusions when they released search queries performed by 65,000 of its users.[132] Even though AOL had anonymized the data by "scrubbing" it of personal information, computer scientists were still able to use that data to identify individual users.[133]

These examples of easy re-identification expose the serious flaws of permitting companies to share anonymized data. They demonstrate that, with the right reference points, the distinction between identifying and anonymized data can be circumvented in order to reveal and exploit personal information. Even though Fitbit states in its Privacy Policy that it contractually prevents its partners from reidentifying user data,[134] it is unclear how effectively Fitbit is able to enforce that policy, and many other companies do not even include such protections in their policies. The line between anonymized and identifying information is particularly crucial in the context of fitness trackers that track information like user locations, activity levels, sleep habits, or heart rates. If personal information can be accessed through anonymized search queries, Facebook likes, Twitter IDs, and Netflix information, it is easy to imagine cross-referencing the anonymized data shared by companies like Jawbone or Basis with other data points in order to reidentify individual users. If computer scientists can predict political leanings, sexual orientation, or emotional stability based on an individual user's Facebook likes,[135] it is highly probable that similar inferences can be made from data gathered by fitness trackers, which measure users' lives in granular detail.

The concerns surrounding reidentified data are further amplified when taken together with users' false sense of security concerning fitness trackers and future unanticipated uses of shared information. Following the current trajectory of current data uses, it is not difficult to imagine a

129. Zetter, *supra* note 126.

130. Anderson, *Pulling Back the Curtain on "Anonymous" Twitterers*, *supra* note 126.

131. *Id.*

132. Bangeman, *supra* note 127.

133. Anderson, *"Anonymized" Data Really Isn't—and Here's Why Not*, *supra* note 126; *see also* Bangeman, *supra* note 127 (reporting that the *New York Times* was even able to use this data to track down searcher no. 4417749, a 62-year-old widow in Georgia).

134. *See* Fitbit *Privacy Policy*, *supra* note 121.

135. Kamdar & Maass, *supra* note 113.

scenario in which "anonymized' data collected and shared by fitness trackers today is reidentified using non-anonymized reference points in the future to create a digital footprint used in employment decisions, insurance benefits, legal proceedings, and other decisions that significantly impact users' lives.

IV. Proposal: Statutory Guidelines for Fitness Trackers Modeled After HIPAA

Fitness trackers present heightened and unique privacy concerns because they collect and transmit the intimate and granular details of users' lives. In the hands of computer scientists, employers, insurance companies, or other entities, this information has the potential to reveal shocking amounts of information about users' health, personality, and behavior. While most laws and privacy policies limit a company's ability to share or sell identifying personal information, researchers have explicitly shown that anonymized data can be cross-referenced with publically available non-anonymized data to identify individual "anonymous" users.[136] These developments have opened the floodgates for unanticipated and insidious uses of data collected by fitness trackers to target and make intimate inferences about individual users.

Even though the information gathered by fitness trackers is not currently protected by HIPAA (unless that information happens to qualify as PHI under HIPAA[137]), it constitutes sensitive information and should be protected as such. Additionally, because users often perceive fitness trackers as harmless accessories, rather than devices that transmit and store huge amounts of revealing health information, regulation is necessary to ensure consumers make effective and informed decisions concerning such devices. In order to adequately protect users' privacy rights against the daunting potential uses of fitness tracker information, Congress should adopt a statutory scheme modeled after HIPPAA (or alternatively, an extension of HIPAA specifically crafted for fitness trackers and health-related mobile applications) with six critical components: (1) Flexibility, (2) Data Minimization, (3) Notice and Control, (4) Limitations on Future Uses, (5) Security, and (6) Data Breach Notification. While none of these components can effectively guard against privacy invasions alone, together they create a comprehensive approach that limits the way health information is gathered and stored by fitness trackers, enables users to

136. *See* Ohm, *supra* note 125, at 716.

137. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 6.

make informed choices about how and when they share fitness information, and protects that information once it has been shared.

A. Flexibility: The Key to Staying Ahead of the Technological Curve

While flexibility is not an explicit feature of this proposed statutory scheme, it is a necessary component of any statutory approach to regulating fitness trackers. The number[138] and variety[139] of fitness trackers is rising, and computer scientists are improving in their ability to reidentify supposedly anonymized data.[140] In order to keep up with the rapidly changing field of fitness trackers, any approach must be flexible enough to adapt to technological and marketplace advances. This can be achieved by establishing broad guidelines similar to those established by HIPAA. Even though HHS is responsible for civil enforcement of HIPAA,[141] as Solove and Winn both recognize, state courts have also used the standards set forth by HIPAA to establish the standard of care in tort cases.[142] A similar approach should apply to fitness trackers. While federal agencies should have the power to enforce fitness tracker regulations, the proposed statute would also explicitly allow state courts to use such regulations to establish the standard of care in common law tort cases. Such an approach would allow the standard set forth by the proposed regulation to evolve in response to technological changes.

B. Data Minimization: Who Can Store What and For How Long?

In order to properly protect fitness tracker information, the proposed statute must limit the collection *and retention* of PFI. Because data collected in aggregate can be used for unforeseen future purposes,[143] Congress should limit the amount of health information gathered and retained by companies that offer fitness trackers to the public. The HIPAA Privacy Rule provides substantial guidance on this subject by requiring covered entities to make reasonable efforts to use and disclose only the *minimum* amount of PHI needed for an intended purpose.[144] Fitness tracker regulation should also require companies to collect only the health

138. *See* Martin, *supra* note 11.

139. *See* Rose, *supra* note 1; Fitbit, *Find Your Fit*, *supra* note 17; Jawbone, *Compare Trackers*, *supra* note 19.

140. *See* Ohm, *supra* note 125, at 716; Anderson, *"Anonymized" Data Really Isn't—and Here's Why Not*, *supra* note 126.

141. U.S. Dep't of Health and Human Servs., *Summary of the HIPAA Privacy Rule*, *supra* note 6; Solove, *supra* note 39, at 106.

142. *See* Solove, *supra* note 69; Winn, *supra* note 69.

143. *See, e.g.*, North, *supra* note 111; Kamdar & Maass, *supra* note 113.

144. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 6.

information required for a particular task or use. The proposed regulation would take this approach a step further by also limiting the retention of data that is no longer necessary for the intended purpose. This would mean that companies would be barred from storing or selling information that is no longer needed "just in case" it may come in handy later for a future unforeseen use. Even though this standard may be difficult to define and apply, establishing such a standard would at the very least put companies on notice that their ability to collect data is not unlimited. While not a complete solution, these limitations would significantly diminish the danger that information gathered today will be used to make important decisions about consumers in the future.

C. Notice & Control: Giving Consumers the Tools They Need in Order to Make Informed Decisions About Sensitive Information.

HIPAA also facilitates users' control over PHI through its Notice, Authorization, and Right of Access requirements.[145] The Notice requirement establishes that covered entities must make their privacy practices known to patients, while the Right of Access and Authorization requirements increase the degree of control patients exercise over their PHI.[146] The proposed statute would include similar provisions to ensure that consumers are adequately informed as to how their data is being used and to safeguard users' ability to exercise effective control over their health information. To achieve this purpose, the statute would explicitly require companies to outline all current uses of data, as well as any anticipated future uses. If companies reserve the right to share or sell de-identified data to third parties, they would also be required to disclose the risks of re-identification to consumers. Companies would also be required to disclose further steps consumers can take to protect their PFI, such as encryption. Moreover, any data uses that are not necessary to the primary use of the device would require users to explicitly "opt-in" to those uses. Finally, the proposed statute would also explicitly prohibit certain uses of PFI, such as using PFI for discriminatory purposes. While such actions may be difficult to prove and may overlap with other areas of law, such as employment law, these regulations would at least send a clear message to companies that certain uses are improper and would help to establish a company's duty to its users. These measures would increase the degree of control users exercise over their PFI and improve consumers' ability to make considered and informed decisions regarding their fitness information.

145. *Id.*
146. *Id.*

D. Security: Protecting Sensitive Information Once It Has Been Shared

Without effective security requirements, any statutory scheme would be unable to adequately protect against privacy invasions that may occur once PFI is shared. Accordingly, the proposed regulation would also include security requirements modeled after the HIPAA Security Rule. The legislation would impose security requirements on all information gathered by fitness trackers and stored by the companies who sell such devices. Like the HIPAA Security Rule,[147] the proposed statute would require companies to (1) ensure the confidentiality of health information collected and stored by fitness trackers (including through encryption); (2) identify and protect against threats to security (both on their servers and in the devices themselves); (3) take reasonable precautions against impermissible uses and disclosures; (4) provide adequate training to its employees and business associates; and (5) ensure compliance by its employees and business associates. These measures would aid in the protection of health information by significantly decreasing the risk of improper disclosures and data breaches.

E. Data Breach Notification: Applying the HITECH Act to Fitness Trackers

The proposed statute would also include data breach and notification requirements modeled after the HITECH Act.[148] Like the HITECH Act, the proposed statute would require companies to notify customers of breaches within 60 days of discovering the breach and notify the media for breaches affecting more than 500 customers. It would also require companies to perform an investigation into how the breach occurred and remedy any gaps in their security or policies as soon as reasonably possible. Assuming a breach does occur, these measures would aid in the protection of PFI by regulating how companies deal with breaches, and by diminishing the risk of future invasions of privacy.

V. Conclusion

Even though the reasonable expectation of privacy has changed significantly since *Katz*, that standard is still alive today in the form of privacy policies and statutes like HIPAA and the FTCA, which protect against the improper disclosure of users' personal information. These measures safeguard consumer privacy by limiting the circumstances in which users' information may be shared with or sold to third parties. The

147. *See* U.S. DEP'T OF HEALTH AND HUMAN SERVS., *HITECH Act Enforcement Interim Final Rule*, *supra* note 54.

148. *Id.*

regulation of fitness trackers is an urgent issue that should be addressed by Congress because fitness trackers are becoming extremely popular and are beginning to be used in new contexts such as employment and insurance coverage.

The fitness tracker statute proposed in this note would fill a statutory gap by providing specific regulation of the PFI collected by fitness trackers. The proposed statute would follow the guidelines for protecting PHI established by HIPAA and adapt them for the purposes of protecting PFI gathered by fitness trackers. Like HIPAA, the statute would be designed to strike a balance between protecting users' fitness information and allowing companies to continue to provide their beneficial fitness tracking services to the public. While the proposed statute will admittedly place some burden on the companies that manufacture and sell fitness trackers, that burden is necessary in order to adequately protect consumers. PFI must be regulated because it has the potential to reveal intimate personal information about users, which, when collected in the aggregate, can be used to make discriminatory or otherwise unfair decisions about consumers without their knowledge. Moreover, regulation is also necessary because users tend to underestimate the privacy concerns associated with fitness trackers. The proposed statute would protect consumers by increasing transparency between customers and companies, provide clear guidelines for companies, increase the security of PFI, and limit the improper use of fitness information.