Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables

MATTHEW R. LANGLEY*

TABLE OF CONTENTS

* Georgetown Law, J.D. 2015; Sonoma State University, B.A. 2012. I would like to thank Professor David Vladeck and Alvaro Bedoya for their assistance in selecting this topic, and Professor Edward Shakin for his guidance in developing this Note. Thank you also to the editors and staff of *The Georgetown Law Journal* for your thoughtful advice throughout the publication process. Lastly, I would like to thank my family and friends, especially my mother, Maureen Fredrickson, without whose unwavering support throughout my education this Note would not have been possible.

INTRODUCTION

Is your heart rate an intentional communication? The answer may not be clear, but what is certain is that the era of consumer wearable devices is upon us.[1] For the first time in history, consumer devices are capable of monitoring sensitive vital sign information, and companies are readily collecting an inordinate amount of individual data.[2] These devices are known as "wearables" and can monitor an individual's heart rate, stress level, brain activity, respiration, body temperature, hydration level, and other related information.[3] Wearables are worn on the wrist, head, ankle, or any other body part, and serve to computerize just about every daily function imaginable. Software can then be used to collect and store these personal health data.[4] As the law currently stands, nothing is stopping health-app companies from selling this collected information to third parties.[5] In the end, individual privacy suffers tremendously when these data are disclosed, and companies are profiting from sensitive health information such as consumers' heart rates.[6]

No federal statute currently addresses the privacy concerns inherent in consumer wearables. When these devices were used for health care or medical purposes, the U.S. Department of Health and the Federal Drug Administration (FDA) were able to set privacy standards. Now that wearables are no longer used strictly for medical purposes, the FDA is restricted and privacy standards for consumer wearables must come from someplace else.

The Electronic Communications Privacy Act of 1986 (ECPA), which serves mainly to limit what information can be disclosed to the government, has the potential to adequately regulate consumer wearables. Unfortunately, the ECPA

---

1. *See* Bill Wasik, *Why Wearable Tech Will Be as Big as the Smartphone*, WIRED (Dec. 17, 2013, 6:30 AM), http://www.wired.com/2013/12/wearable-computers/all/ ("It may seem laughable to suggest that people will soon neglect their iPhones in favor of amped-up watches, eyeglasses, rings, and bracelets. But then again, 10 years ago it seemed laughable to think that people would use their smartphones to email, surf the web, play games, watch videos, keep calendars, and take notes—all once core tasks of desktop PCs.").

2. *See* Morgan Brown, *What's Next for Wearable Technology and What It Means for Health Data*, TRUEVAULT (July 28, 2014), https://www.truevault.com/blog/whats-next-wearable-tech-health-data.html#.VJJy-4Vzj0A.

3. *See* David Talbot & Kyanna Sutton, *Making Stretchable Electronics*, MIT TECH. REV. (Aug. 21, 2012), http://www.technologyreview.com/demo/428944/making-stretchable-electronics/.

4. *See* Brown, *supra* note 2.

5. "[Health] apps include those that support diet and exercise programs; pregnancy trackers; behavioral and mental health coaches; symptom checkers that can link users to local health services; sleep and relaxation aides; and personal disease or chronic condition managers." *Fact Sheet 39: Mobile Health and Fitness Apps: What Are the Privacy Risks?*, PRIVACY RTS. CLEARINGHOUSE (Dec. 1, 2014), https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks#section%202.

6. *See id.*

was enacted in 1986 and did not contemplate modern communication technology. Moreover, there is a loophole in the ECPA that allows companies to freely disclose customer records, but not contents of a communication, to third parties.[7] Based on the current statutory language of the ECPA, it is likely that most health data would be classified as customer records instead of contents of a communication.[8] Modernizing the ECPA could solve the commercial wearable problem by including sensitive health data in its statutory definition of content.

It is important to note at the outset that wearables may only be one part of the privacy puzzle. Technology is advancing at an exponential rate and no one knows what methods of communication will be available in the future. This Note proposes that amending the ECPA can solve the problem of consumer wearables with regard to protecting the privacy of health information collected from such devices and later sold to third parties. The wearables problem must be addressed immediately before privacy becomes but a distant memory in an amorphously digital world.[9]

Part I will introduce the concept of consumer wearables and expand on the privacy concerns such devices create. Part II will explain why the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the FDA lack jurisdiction over such devices. Part III will introduce the relevant statutes and discuss their application to health data, arguing that analogizing health data with customer records, as opposed to contents of a communication, will be problematic. Finally, Part IV proposes an amendment to the Stored Communications Act (SCA) that encompasses sensitive health data in its definition of contents.

I. WEARABLE TECHNOLOGY: A NEW ERA OF PRIVACY CONCERNS

A. CONSUMER WEARABLES ALLOW INDIVIDUALS TO COMMUNICATE THEIR PERSONAL HEALTH DATA

Wearable technology is exactly what it sounds like—computerized clothing or accessories that can be comfortably worn on the user's body.[10] Wearables can come in many different forms including watches, glasses, belts, shirts, shoes, and jewelry.[11] These devices are able to perform many of the same functions as mobile phones and laptops, but "create constant, convenient, seamless, portable,

7. *See* 18 U.S.C. § 2702(c)(6) (2012); *see also infra* note 113 and accompanying text.

8. *See infra* Part III.B.2.

9. Some examples of future individual privacy issues may include biometric data and facial recognition. *See* Andrea Peterson, *The Biometrics Revolution Is Already Here—And You May Not Be Ready for It*, WASH. POST (Oct. 17, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/17/the-biometrics-revolution-is-already-here-and-you-may-not-be-ready-for-it/.

10. Kiana Tehrani & Andrew Michael, *Wearable Technology and Wearable Devices: Everything You Need to Know*, WEARABLE DEVICES MAG., http://www.wearabledevices.com/what-is-a-wearable-device/ (last updated Mar. 26, 2014).

11. *See* Joanna Stern, *Where to Wear Your Technology? Torso to Toe*, WALL ST. J. (Jan. 7, 2014, 6:41 PM), http://www.wsj.com/articles/SB10001424052702304617404579306551647751522.

and mostly hands-free access to electronics and computers."[12] Unlike handheld devices, wearable devices can monitor and record physical activity and sensitive health information—such as a user's heart rate, skin temperature, or respiratory rate—in real time.[13] Wearables are also more efficient than smartphones because they do not require a user to reach into his pocket, grab a phone, type a password, and then access an app.[14] Wearables never have to be removed and can be worn during sleep, exercise, and showers.[15]

Although wearables are becoming more functional, these devices were, and continue to be, commonly used in the medical field. In addition to a patient's personal description of his own symptoms, doctors prescribe blood-pressure monitors, heart-rate monitors, stress detectors and other wearable devices in order to provide a deeper understanding of their patients' health.[16] As discussed in Part II, federal statutes and regulations are capable of addressing the privacy concerns inherent in these health-related devices, at least as far as the medical field is concerned.

Now the market is being flooded with consumer wearables that have little to do with medical necessity.[17] The features of these devices differ, but most have a common goal—to recreationally track health and fitness levels. Take Apple's new Apple Watch for example.[18] The Apple Watch contains a sensor that detects the wearer's heart rate and constantly monitors his physical activity and health.[19] The goal of this feature is to provide a "complete picture of [the user's] all-day physical activity."[20] At the click of a button, the wearer can even share his heart rate with another wearer.[21] However, it should be noted that the watch keeps track of the wearer's heart rate at all times, not just when the wearer intends to share it.

The widespread increase of wearables in the market is not conjectural: according to a study conducted by PricewaterhouseCoopers's Health Research

---

12. Tehrani & Michael, *supra* note 10.

13. *See* David Pogue, *Wearable Devices Nudge You to Health*, N.Y. TIMES, June 26, 2013, at B1; *see also* Nick Statt, *Wearable Tech's Most Important Race: Turning Heartbeats into Cash*, CNET (Nov. 11, 2014, 4:00 AM), http://www.cnet.com/news/wearable-tech-most-important-race-turning-heartbeats-into-cash/.

14. *See* Wasik, *supra* note 1.

15. *See* Pogue, *supra* note 13.

16. *See* Jess Bolluyt, *What Can Wearable Devices Really Do?*, WALL ST. CHEAT SHEET (Aug. 29, 2014), http://wallstcheatsheet.com/technology/what-are-wearable-devices-really-capable-of.html/?a=viewall; *see also* Nilesh Chandra & Chris Steel, *Wearable Tech Regulated as Medical Devices Can Revolutionize Healthcare*, MED. DEVICE & DIAGNOSTIC INDUS. (June 18, 2014), http://www.mddionline.com/article/wearable-tech-regulated-medical-devices-can-revolutionize-healthcare-6-18-2014.

17. Some brands include the Fitbit, Apple Watch, Jawbone UP, Nike+ FuelBand, and Motorola's Moto 360.

18. Readers should note that the Apple Watch is merely being used as an example, and that what can be said about the Apple Watch can also be said about many wearables.

19. *See The Watch Is Here*, APPLE, https://www.apple.com/watch/features/ (last visited Dec. 18, 2014).

20. *Id.*

21. *See Technology*, APPLE, https://www.apple.com/watch/technology/ (last visited Dec. 18, 2014).

Institute, nearly 7.6 million wearables were shipped within the United States alone in 2014.[22] These numbers represent a 200 percent increase from the amount shipped in the previous year.[23] Additionally, roughly one-in-five U.S. consumers own a wearable device.[24] These numbers are expected to rise as technological advancements and increased competition lead to more affordable prices.[25]

Undoubtedly, wearables represent a huge step in the development of technology. These devices, paired with health apps, allow users to track their daily activities and fitness progressions in order to live healthier lifestyles. Sleep patterns, calories burned, running speed, and steps taken in a day all can be calculated without any further action by the user.[26] But this convenience does not come without a price.

B. WITHOUT ADEQUATE LEGAL STRICTURES IN PLACE, HEALTH-APP COMPANIES ARE FREE TO SELL PERSONAL HEALTH DATA OBTAINED THROUGH WEARABLES

Wearables allow health apps to observe consumer action on a more detailed level and enable these companies to collect personal information.[27] "People are now tracking every facet of their lives with the aid of technology," and this includes sensitive health information.[28] When wearable medical devices were introduced to the health sector, patient information became more accessible and portable.[29] Patients had a concern that someone other than their health care provider could see this information, but this concern was minimal because disclosure of patient information was limited.[30] Now that consumers can use wearables for nonmedical purposes, their personal information is being collected, stored, and transmitted freely.

Generally, wearables collect data about the user and then wirelessly send that information to a smartphone app.[31] Those data are usually then sent to the cloud

---

22. PWC HEALTH RESEARCH INST., HEALTH WEARABLES: EARLY DAYS 9 (2014), *available at* http://www.pwc.com/en_US/us/health-industries/top-health-industry-issues/assets/pwc-hri-wearable-devices.pdf.

23. *Id.*

24. *Id.* at 1.

25. It is estimated that in 2014, nearly fifty-two million wearable devices were shipped globally. Paul Lamkin, *Wearable Tech Sales to Top 50 Million by the End of the Year*, WEARABLE NEWS (Nov. 6, 2014), http://www.wareable.com/wearable-tech/wareable-tech-sales-to-top-50-million-in-2014-445.

26. *See* Bolluyt, *supra* note 16.

27. *See* Avi Goldfarb & Catherine Tucker, *Privacy and Innovation* 3 (Nat'l Bureau of Econ. Research, Working Paper No. 17124, 2011), http://www.nber.org/papers/w17124.pdf.

28. MARIO BALLANO BARCENA ET AL., SYMANTEC SECURITY RESPONSE: HOW SAFE IS YOUR QUANTIFIED SELF? 4 (2014), *available at* https://www.blackhat.com/docs/eu-14/materials/eu-14-Wueest-Quantified-Self-A-Path-To-Self-Enlightenment-Or-Just-A-Security-Nightmare-wp.pdf (internal quotation marks omitted).

29. *See* FED. TRADE COMM'N, SPRING PRIVACY SERIES: CONSUMER GENERATED AND CONTROLLED HEALTH DATA (2014), *available at* http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf#page=22.

30. *See id.*

31. *See* Ruby A. Zefo, *Wearable Devices: Keep Data Privacy in Check*, INFO.WK. (Aug. 18, 2014, 12:06 PM), http://www.informationweek.com/mobile/mobile-devices/wearable-devices-keep-data-privacy-in-check/a/d-id/1298085.

to be stored or analyzed.[32] In many respects, those datas' value is based on their potential to be used for the greater good, such as disease prevention.[33] From a commercial standpoint, marketers want these data to gain insight into individual preferences as a means of offering personally targeted products.[34] A sports equipment manufacturer, for example, could collect an individual's heart rate data, learn that the user is increasing activity and losing weight, and then send an offer for tighter fitting clothes. Additionally, tracking a user's sleep patterns could lead to a timely brochure from a mattress company.[35] "In today's world, where information is the real currency, [wearables] are potential goldmines ripe for exploitation."[36]

According to Federal Trade Commission (FTC) findings, health apps are in fact transmitting sensitive health information to third parties.[37] On May 7, 2014, the FTC released a study of twelve different health and fitness apps.[38] The study found that those apps transmitted user data to seventy-six different third parties, including advertisers.[39] The information transmitted varied all the way from device information to exercise routines, dietary habits, and symptom searches.[40] In a few instances, even names and addresses were being transmitted.[41] Although the FTC did not reveal the names of the apps it studied, the study shows that wearable privacy concerns are not just theoretical.[42]

The privacy risks involved in collecting data through wearables are substantial. Returning to the Apple Watch example, a user is free to send his heart rate to a friend; that action is intentional. However, at all other times when the user is wearing the watch, heart rate data are still being captured and transmitted to the health app to be stored and analyzed.[43] The health-app company can receive an unprecedented amount of sensitive information about the individual and is

32. *Id.*
33. *Id.*
34. *See id.*
35. *See* BARCENA ET AL., *supra* note 28, at 8.
36. *Id.*
37. *See* FED. TRADE COMM'N, *supra* note 29.
38. *See id.*
39. *Id.*
40. *Id.*
41. *See* Kate Kaye, *FTC: Fitness Apps Can Help You Shred Calories—and Privacy*, ADVERT. AGE (May 7, 2014), http://adage.com/article/privacy-and-regulation/ftc-signals-focus-health-fitness-data-privacy/293080/.
42. *See* Jah-Juin Ho, N.J. Office of Att'y Gen., Address at the Federal Trade Commission Spring Privacy Series on Consumer Generated and Controlled Health Data: A Snapshot of Data Sharing 24 (May 7, 2014) (transcript available at http://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf) ("This project was meant to be a small snapshot in time, so we looked at two daily activity apps connected to wearables, two exercise apps, two dietary and meal apps, three symptom checker apps, one pregnancy app, one diabetes app, and one smoking cessation app.").
43. Granted, the user could always take off the wearable, but will be left with an unfortunate ultimatum—either stop using the device or succumb to lack of privacy. This choice would run contrary to the key appeal of a wearable—never having to take it off.

free to sell those data to third parties.[44] Through the advent of smartphones and other mobile devices, companies have been able to collect sensitive information from their customers.[45] Location, political preferences, communications with contacts, search queries about health conditions, and many other types of sensitive information are collected and sold.[46] Now that wearables have entered the market, a whole new world of sensitive information is available to these companies.

Although giving companies more information about ourselves may be seen as beneficial to some, there are obvious privacy implications. Soon, companies will be able to use undisclosed personal health data as a basis for making life-changing determinations. For example, having a relatively inactive week may potentially cause an individual to be deemed a "health risk" in the eyes of his or her insurance provider.

II. INAPPLICABILITY: CONSUMER WEARABLES DO NOT FIT WITHIN THE CURRENT HEALTH-RELATED REGULATORY SCHEMES

It is clear that consumer wearables present a new problem in the field of health data privacy. Unfortunately, no federal statute currently regulates the sale of information obtained through wearables. Additionally, now that wearables are being used as consumer products instead of purely medical devices, HIPAA and the FDA are unable to provide effective regulatory oversight.

A. HIPAA'S PRIVACY PROTECTIONS DO NOT APPLY TO HEALTH APPS

"Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private."[47] Congress essentially codified the famous Hippocratic Oath when it passed HIPAA.[48] One of the most basic aspects of HIPAA is that it aimed to protect the privacy of an individual's personal health information by limiting disclosure.[49] As will be explained, HIPAA solved the privacy problem of wearables in the medical field, but remains an ineffective source of protection in the commercial sphere.

HIPAA was enacted, in part, to ensure confidentiality in all health care information.[50] To reach its goal, HIPAA required the Department of Health and

---

44. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 2 (2013), *available at* http:/ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

45. *See id*.

46. *See id*.

47. *The Hippocratic Oath*, NAT'L LIBR. OF MED. & NAT'L INST. OF HEALTH, http://www.nlm.nih.gov/hmd/greek/greek_oath.html (Michael North trans.) (last updated Feb. 7, 2012).

48. *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

49. *See* Susan M. Gordon, *Privacy Standards for Health Information: The Misnomer of Administrative Simplification*, 5 DEL. L. REV. 23, 23 (2002).

50. *See Health Information Privacy*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/ (last visited Nov. 20, 2014).

Human Services to adopt standards relating to the "electronic exchange, privacy, and security of health information."[51] As a whole, these regulations are known as the "Administrative Simplification" provisions.[52] One of these provisions, the Privacy Rule, regulates the use and disclosure of protected health information by covered entities and defines "protected health information" as "individually identifiable health information."[53] Once an organization is deemed a covered entity under HIPAA, numerous safeguards protect all individually identifiable health information data that it maintains or transmits.[54] Additionally, the Health Information Technology for Economic and Clinical Health Act (HITECH Act), passed as part of the American Recovery and Reinvestment Act of 2009, expanded the jurisdictional element of HIPAA to include "business associates" of covered entities.[55]

Although HIPAA safeguards for personal health information are extensive, the protections only apply to wearables if health apps are considered "covered entities."[56] Covered entities can only be (1) a health plan,[57] (2) a health care clearinghouse,[58] or (3) a health care provider who transmits any health information in electronic format.[59]

At least for purposes of consumer wearables, health apps are not covered entities. Health apps do not provide medical care, transmit information between entities in the health care system, or provide health care services. These apps just allow individuals to collect data through their wearables for personal use. Therefore, because consumer wearable health apps are not covered entities, HIPAA does not regulate them.

HIPAA may have solved the privacy problem of wearables in the health sector by limiting covered entities' disclosure of patient information, but it is

---

51. *See Health Insurance Portability & Accountability Act*, N.H. DEP'T OF HEALTH AND HUM. SERVS., http://www.dhhs.state.nh.us/oos/hipaa/index.htm (last visited June 23, 2015).

52. *Id.* (internal quotation marks omitted).

53. *See* 45 C.F.R. §§ 160.102–.103 (2015); *see also* Stacey A. Tovino, *The Use and Disclosure of Protected Health Information for Research Under the HIPAA Privacy Rule: Unrealized Patient Autonomy and Burdensome Government Regulation*, 49 S.D. L. REV. 447, 450–53 (2004).

54. For the reasons listed in this section, health apps used on consumer wearables are not covered entities under HIPAA. Therefore, a detailed analysis of HIPAA's privacy protections would be distracting to this section's purpose. For an overview of HIPAA's safeguards, see Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. FED. 133 (2004).

55. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 §§ 13001, 13401, 13404; s*ee also* Jason W. Davis, *HITECH HIPAA Amendments: New Rules on Breach Notification, Business Associate Compliance, and Enforcement*, 21 HEALTH LAW. 23 (2009).

56. *See* 45 C.F.R. § 160.102 (2015).

57. A health plan is "an individual or group plan that provides, or pays the cost of, medical care." 45 C.F.R. § 160.103 (2015).

58. A "health care clearinghouse" is a complicated term, but essentially involves an entity that transmits information—typically claims and billing information—between other entities in the health care system. *See id.*; *see also Patient's Guide to HIPAA*, WORLD PRIVACY F. (Sept. 18, 2013), http://www.worldprivacy forum.org/2013/09/hipaaguide9-2/.

59. Health care providers are persons or entities that furnish, bill, or are paid for health care services. *See* 45 C.F.R. § 160.103 (2015).

completely ineffective against consumer wearables. Without a covered entity involved, information such as a person's heart rate, physical activity, and sleep patterns is not protected health information.[60] There is a statutory difference between health data collected as part of a HIPAA-covered entity and health data collected by an individual with a consumer wearable.[61] As long as the health data are not stored and shared with any HIPAA-covered entity or business associate, the exchange of that data are not susceptible to HIPAA regulations at all.[62] When it comes to protecting the privacy of consumer health data, HIPAA is not the answer.

B. THE FDA WILL NOT REGULATE CONSUMER WEARABLES OR THEIR ASSOCIATED HEALTH APPS

Mobile health technology is undoubtedly in the crosshairs of the FDA. Through the Food, Drug, and Cosmetic Act, the FDA has broad jurisdiction over medical "devices," which are defined as any product "intended for use in the diagnosis[,] . . . treatment, or prevention of disease," or "intended to affect the structure or any function of the body."[63] This definition limits the FDA because any regulation it implements would only apply to medical devices. Thus, the FDA can only regulate consumer wearables if they meet the statutory definition of medical devices.

Whether consumer wearables, or their associated health apps, meet the umbrella definition of medical devices depends on their "intended use."[64] A product intended to diagnose or treat a condition is considered a medical device, whereas a product intended to promote or encourage general health or wellness is not considered a medical device.[65] Unfortunately, the distinction between the two is not always clear. For instance, an overweight person may use a consumer wearable to assist with exercise and weight management, but could also use it to treat the medical condition of obesity.[66] To help clarify the distinction, FDA regulations define "intended use" as the "objective intent of the persons legally responsible for the labeling of devices," which can be shown through "labeling claims, advertising matter, or oral or written statements."[67] A majority of consumer wearables are advertised to promote health, not to treat medical

60. *See id*.

61. *See* Morgan Brown, *What Developers Need to Know about HIPAA Compliance in Wearable Tech*, TRUEVAULT (May 14, 2014), https://www.truevault.com/blog/what-developers-need-to-know-about-hipaa-compliance-in-wearable-tech.html#.VG7p1oVzj0A.

62. *See id*.

63. 21 U.S.C. § 321(h)(2)–(3) (2012).

64. *See* Vincent J. Roth, *The mHealth Conundrum: Smartphones & Mobile Medical Apps—How Much FDA Medical Device Regulation Is Required?*, 15 N.C. J.L. & TECH. 359, 371–72 (2014).

65. Scott D. Danzis & Christopher Pruitt, *Rethinking the FDA's Regulation of Mobile Medical Apps*, 9 SCITECH LAW. 1, 2 (2013), *available at* http://www.cov.com (follow "Publications" hyperlink; then choose "Danzis" as author; then follow "Rethinking" hyperlink).

66. *See* Roth, *supra* note 64, at 372.

67. 21 C.F.R. § 801.4 (2015).

conditions, so it is highly unlikely that the FDA will treat them as medical devices.[68]

Although consumer wearable devices themselves are likely exempt from current FDA regulations, the FDA could still potentially choose to regulate the health-app companies that provide software for wearables. On September 25, 2013, the FDA responded to the market increase of mobile medical apps and provided final guidance as to how the FDA would regulate mobile medical apps in the future.[69] According to this final guidance, apps will be regulated if they are intended "[1] to be used as an accessory to a regulated medical device; or [2] to transform a mobile platform into a regulated medical device."[70] By adding the word "intended" before these two categories, the final guidance limits the types of mobile medical apps that will be regulated.[71] The FDA will be unwilling to regulate the health apps used on wearables because they are predominantly intended to promote health, not for medical purposes.[72]

The FDA's primary purpose is to protect public health, not to safeguard individual privacy.[73] Regulating medical devices is necessary to maintain individual health and safety because defective devices could cause serious injury or death to the consumers who rely on them.[74] The same concerns are not apparent in consumer wearables because there is no diagnosis component. Primarily, wearables will just track an individual's heart rate recreationally instead of using that information to prescribe a medical diagnosis. Although the FDA could potentially regulate in this arena by expanding the definition of medical devices, its final guidance suggests that it is unwilling to regulate purely commercial products. Thus, at least for the foreseeable future, relying on the FDA is not a viable solution to the privacy problem of consumer wearables.

---

68. *See, e.g.*, *Who We Are*, FITBIT, http://www.fitbit.com/about (last visited Dec. 18, 2014) ("We're a passionate team dedicated to health and fitness who are building products that help transform people's lives. While health can be serious business, we feel it doesn't have to be. We believe you're more likely to reach your goals if you're encouraged to have fun, smile, and feel empowered along the way.").

69. *See* U.S. DEP'T OF HEALTH & HUM. SERVS. FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2013), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

70. *Id*. at 7.

71. *See id*.

72. *See, e.g.*, *Who We Are*, *supra* note 68.

73. *See What We Do*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/AboutFDA/WhatWeDo /default.htm (last updated Aug. 5, 2014) ("FDA is responsible for protecting the public health by assuring the safety, efficacy and security of human and veterinary drugs, biological products, medical devices, our nation's food supply, cosmetics, and products that emit radiation.").

74. *See* Alex Krouse, Note, *iPads, iPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices*, 9 IND. HEALTH L. REV. 731, 746 (2012).

III. INADEQUACY: THE ECPA APPLIES TO HEALTH APPS, BUT DOES NOT LIMIT THEIR ABILITY TO DISCLOSE PERSONAL HEALTH DATA TO THIRD PARTIES

A. A BRIEF PRIMER: ENACTING THE SCA PROVISIONS OF THE ECPA

The Fourth Amendment served as a key player in early attempts to protect the privacy of communications. In 1967, the Supreme Court in *Katz* held that the Fourth Amendment protects "people, not places" and that the government needed a search warrant before it could obtain the contents of a telephone conversation.[75] *Katz* also suggested that the critical inquiry in determining whether the Fourth Amendment was violated is whether the individual had a reasonable expectation of privacy in the communication.[76] Congress immediately responded by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), which created a statutory right to privacy for oral communications that passed through a wire.[77] Title III required police to obtain a warrant before intercepting these types of communications.[78] However, Title III was limited and the Fourth Amendment's reasonable expectation of privacy test continued to govern nonoral communications.

In 1979, the Supreme Court distinguished between the contents of a communication and other attributes, such as the communication's source, destination, and duration.[79] The *Smith* Court held that on the one hand, a person has a reasonable expectation of privacy in the contents of private phone conversations, but on the other hand, has no reasonable expectation of privacy in the customer records of the telephone numbers dialed.[80] Police access of customer records would not be a search under the Fourth Amendment because a customer's dialing information is volunteered to the telephone company.[81] The Court in effect preserved Fourth Amendment protections for content, and removed constitutional protections from noncontent such as customer records. However, if Congress had wanted to make a law protecting noncontent, it was free to do so.[82]

By 1986, the Internet infiltrated the business world, and the use of e-mail brought about concerns for the security of company data.[83] Confidential information, which had been relatively protected on personal computers, was now being

---

75. *See* Katz v. United States, 389 U.S. 347, 351, 357 (1967).

76. *See id.* at 362 (Harlan, J., concurring).

77. *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communication Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1561–62 (2004).

78. *See id*.

79. *See* Smith v. Maryland, 442 U.S. 735, 743 (1979); David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1, 6 (2003).

80. *Smith*, 442 U.S. at 743–46 ("When [petitioner] used his phone, [he] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

81. *See id*. at 745–46.

82. *See* Phillips, *supra* note 79, at 1, 6–7.

83. *See* Mulligan, *supra* note 77, at 1559–60.

sent via e-mail.[84] Although this activity posed a problem for businesses, it is likely that individual consumers were not too concerned: in 1984, only about five percent of households owned a computer.[85] Regardless, in an abundance of caution, Congress sought to provide appropriate privacy protections for this growing trend of Internet activity by enacting the Electronic Communications Privacy Act of 1986 (ECPA).[86] The ECPA codified protections for electronic communications and extended privacy protections to e-mail and information stored by third parties. [87] The ECPA was further broken down into three statutes, including the Stored Communications Act (SCA), which established rules about when entities may disclose their customers' communications or records.[88] The SCA provides the answer to the consumer wearable privacy problem.

B. THE SCA LIMITS CERTAIN SERVICE PROVIDERS FROM DISCLOSING THE CONTENTS OF COMMUNICATIONS, BUT DOES NOT PREVENT DISCLOSURE OF CUSTOMER RECORDS

An overwhelming majority of the literature and case law pertaining to the SCA deals with section 2703. Section 2703 provides the rules that the government must follow in order to compel a provider to disclose information about its customers involuntarily.[89] With regard to content, the government must obtain either a search warrant, subpoena, or "2703(d) order" to compel disclosure of the information.[90] With respect to noncontent records, the government can compel disclosure through a warrant, a 2703(d) order, consent of the customer, or by submitting a written request to the provider.[91] Section 2703 is an important check on the government's power to compel disclosure, but that is not the main focus of this Note.

Section 2702 governs when a provider can voluntarily disclose information to commercial third parties,[92] stating that a person or entity providing an "electronic communication service" or a "remote computing service" to the public shall not knowingly divulge the contents of that communication, subject to the

84. *See id*. at 1560.

85. *See id*.

86. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

87. Mulligan, *supra* note 77, at 1558.

88. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012); Wiretap Act, 18 U.S.C. §§ 2511–2522 (2012); Pen Register Act, 18 U.S.C. §§ 3121–3127 (2012).

89. *See* 18 U.S.C. § 2703 (2012); *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1219 (2004).

90. *See* Kerr, *supra* note 89, at 1219 ("[A 2703(d) order] is something like a mix between a subpoena and a search warrant. To obtain the order, the government must provide 'specific and articulable facts showing that there are reasonable grounds to believe' that the information to be compelled is 'relevant and material to an ongoing criminal investigation.' . . . The order is then served like an ordinary subpoena . . . .").

91. *Id*.

92. *See* 18 U.S.C. § 2702 (2012). This statute also governs when entities can voluntarily disclose information to the government. *Id.*

exceptions listed in section 2702(b).[93] Section 2702(c) distinguishes content from customer records and provides less stringent rules for voluntary disclosure of customer records.[94]

With this overview in mind, the SCA's applicability to consumer wearables will depend on two determinations. First, the SCA will only apply to the associated health apps if they provide either an electronic communication service or a remote computing service to the public. Second, if the health apps provide one of these services, the level of protections afforded to the wearable's communications will depend on whether the communications are considered content or noncontent.

1. As Either an Electronic Communication Service or a Remote Computing Service, Health Apps Are Regulated by Section 2702 of the SCA

In order for section 2702 to apply, the health data app must provide either an electronic communication service or a remote computing service to the public.[95] Those providers who do not provide an electronic communication service or a remote computing service to the public are free to disclose information without violating the SCA.[96] For the following reasons, it is likely that a court would find that health apps provide either an electronic communication service or a remote computing service, and are therefore regulated by section 2702.

For purposes of the SCA, an electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[97] The first step in deciding whether an entity provides an electronic communication service is to look at the nature and context of the communication involved.[98] The focus should be on the provider's role with respect to that particular communication, as opposed to the provider's primary business purpose or function.[99] If the entity provides the ability to send or receive a particular type of communication, then the entity will be a provider of an electronic communication service with respect to that particular communication.

The SCA defines a remote computing service as "the provision to the public of computer storage or processing services by means of an electronic communications system."[100] An electronic communications system is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related

93. *Id*. For a list of the section 2702(b) exceptions, see *infra* notes 110–12 and accompanying text.
94. *Id*.
95. *Id*.
96. *See* Kerr, *supra* note 89, at 1220.
97. 18 U.S.C. § 2510(15) (2012).
98. *See* Kerr, *supra* note 89, at 1215–16.
99. *See id*.
100. 18 U.S.C. § 2711(2) (2012).

electronic equipment for the electronic storage of such communications."[101] The term "computer storage" is both facially ambiguous and undefined in the SCA.[102] However, the SCA's legislative history states that, generally speaking, a remote computing service provides an off-site computer that stores or processes data for a customer.[103]

A remote computing service comes with two further limitations. First, the storage of information cannot be merely incidental to the main service provided by the remote computing service. "For example, an airline may compile and store passenger information and itineraries through its website, but these functions are incidental to providing airline reservation service, not data storage and processing service; they do not convert the airline into a [remote computing service]."[104] Second, a service can only be a remote computing service if it provides its services to the public at large, whether for free or for cost.[105] If anyone can sign up and/or pay for an account, then that service is provided to the public.[106] If, on the other hand, a provider makes its remote computing service available only to those whom it has a special relationship with, it will not be considered a provider "to the public."[107]

Health apps provide wearable users with both an electronic communication service and a remote computing service. When an individual uses the Apple Watch to voluntarily communicate heart rate data to a friend, the health app is functioning as an electronic communication service; clearly this is an electronic communication, and the health app is providing the ability to send the user's

---

101. 18 U.S.C. § 2510(14) (2012).

102. The term "processing services" is also facially ambiguous and lacks a definition in the SCA. The legislative history suggests that a processing service involves outsourcing functions. *See* S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. Professor Kerr uses eBay as an example of how processing service is a tricky concept. The key might be the "outsourcing function," but "[a]t a literal level, . . . it seems at least possible to conclude that eBay provides [a remote computing service]. Every website processes information sent to it, and eBay is no exception. If I bid for an item listed on eBay, eBay's computers take in my bid and calculate whether it is the highest bid, taking my bid if it is the highest bid or rejecting it if there are higher ones. In this limited sense, eBay is performing a processing service. . . . But there are no decided cases on how to construe the phrase 'processing services' in the SCA, so the answer at least today remains ambiguous." Kerr, *supra* note 89, at 1230–31.

103. *See* S. REP. NO. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564–65. A common example of a computer that stores data is a server that allows users to store data for future retrieval.

104. *See* H. MARSHALL JARRETT ET AL., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 119 (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [hereinafter DOJ MANUAL] (citing *In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 310 (E.D.N.Y. 2005)).

105. *See* Kerr, *supra* note 89, at 1226 (citing Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998)).

106. "It may seem odd at first that a service [such as Verizon] can charge a fee but still be considered available 'to the public,' but this approach mirrors commercial relationships in the physical world. For example, movie theaters are open 'to the public' because anyone can buy a ticket and see a show, even though tickets are not free." DOJ MANUAL, *supra* note 104, at 120.

107. *Id*. Likewise, if an employer or university provides e-mail accounts to its employees or students, those e-mail accounts are not available to the public. In these contexts, the provider offers the user an account because the provider has a special relationship with the user. *Id*.

heart rate data to a friend. When the wearable is merely collecting heart rate data from the user, it is functioning as a remote computing service; the health app is available to anyone with a wearable, its main function is to track heart rate data, and it stores and processes data for the user.[108] There is a debate about whether a company can be a provider of both an electronic communication service and a remote computing service, but for the purpose of applicability to wearables all that matters is that health apps provide at least one or the other.[109]

2. The SCA Treats Personal Health Data Obtained Through Wearables as Customer Records Instead of Content

The disclosure rules applicable to the data obtained through wearables depend on whether the communications are content or noncontent. Assuming that there is an electronic communication service or a remote computing service to the public, the provider is not allowed to voluntarily divulge the contents of a communication to any person or entity unless one of the exceptions outlined in section 2702(b) applies.[110]

Four of the 2702(b) disclosure exceptions are straightforward: a provider can divulge the contents of a communication if it is necessary to the delivery of the communication (exceptions one and four), if the law so requires (exception two), or with the consent of the person whose rights are at stake (exception three).[111] The remaining exceptions involve specific instances where privacy rights give way to government interests.[112]

---

108. Note that the SCA specifically states that electronic communications do not include communications from a "tracking device" (which is further defined as an "electronic or mechanical device which permits the tracking of the movement of a person or object"). 18 U.S.C. § 2510(12)(C) (2012); 18 U.S.C. § 3117(b) (2012). Taken literally, this definition appears to include wearables. However, the case law makes clear that section 3117(a) limits tracking devices to those devices that are installed by the government. *See* United States v. Powell, 943 F. Supp. 2d 759, 777 (E.D. Mich. 2013) ("Moreover, a cell phone is not a 'tracking device' as defined by 18 U.S.C. § 3117. First, a cell phone is not a government-owned-and-installed device. Instead, it is a personal communications device that an individual purchases and owns. The statutory language of [section] 3117 specifically contemplates government installation: '[i]f a court is empowered to issue a warrant or other order for the *installation* of a mobile tracking device . . .'" (alteration in original) (citing 18 U.S.C. § 3117(a))); *see also In re* Application of the United States for an Order, 411 F. Supp. 2d 678, 681 (W.D. La. 2006) ("Tracking devices are devices that are 'installed' at the request of the Government.").

109. The Ninth Circuit holds that while a company may provide both an electronic communication service and a remote computing service as an entity, it can only provide one or the other to an individual customer. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902–03 (9th Cir. 2008). At least one court rejected the Ninth Circuit's approach and held that a company can be a provider of both an electronic communication and a remote computing service to the same customer. Under this approach, whether the provider is an electronic communication service or a remote computing service depends on what role the provider has played or is playing with respect to the particular communication in question. *See* DOJ MANUAL, *supra* note 104, at 120 (citing Flagg v. Detroit, 252 F.R.D. 346, 362 (E.D. Mich. 2008)).

110. 18 U.S.C. § 2702(b) (2012).

111. *Id.*; *see also* Kerr, *supra* note 89, at 1221.

112. 18 U.S.C. § 2702(b). A provider can divulge contents when it believes there is an emergency (exception eight), if the contents were inadvertently obtained by the provider and they relate to a crime

There are not many differences between the disclosure rules of content and noncontent, but one important difference is directly relevant to wearables. According to section 2702(c)(6), a provider "may divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any person other than a governmental entity" without restriction.[113] If wearable data are considered noncontent, then health apps would not run afoul of section 2702 by selling the data without notifying the individual or obtaining his consent. On the other hand, if wearable data are considered content, they will receive the limited disclosure protections of section 2702(b). Unfortunately, as will be discussed in this section, health data obtained through wearables blur the line between content and noncontent. Thus, it brings up the difficult question of whether a user's heart rate obtained through a wearable is the content of a communication or is more like a customer record.

For purposes of the ECPA, "contents, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."[114] Unfortunately, the words "substance, purport, or meaning" are not further defined in the statute. It has been suggested that "content" refers to communications that a person wishes to share with another person.[115] Thus, the body of an e-mail, the subject line of the e-mail, or anything with a substantive message would be considered content.[116] Stored e-mails, voicemails, or word processing files stored in employee network accounts would also be considered content.[117]

Noncontent—which includes customer records—is not expressly defined in the ECPA, but is described as being the "information *about* the communication that the network uses to deliver and process the [actual substantive message]."[118] When the ECPA amended the Federal Wiretap Act in 1986, it deleted the phrase "identity of the parties or the existence of the communication" from the definition of content.[119] Therefore, noncontent was negatively defined as any information not concerning the substance, purport, or meaning of the communication at issue, and included the existence of the communication and the identities of the parties involved. For example, account usage, mail header information (minus the subject line), history of outgoing e-mail addresses sent

---

(exception seven), if necessary to protect the provider's rights or property (exception five), or if a provider finds child pornography and must disclose it to the police (exception six). *See* Kerr, *supra* note 89, at 1221–22.

113. 18 U.S.C. § 2702(c)(6).

114. 18 U.S.C. § 2510(8) (2012) (internal quotation marks omitted). The definitions in section 2510 apply to section 2702. *See* 18 U.S.C. § 2711(1) (2012).

115. *See* Kerr, *supra* note 89, at 1228.

116. *Id.*

117. DOJ MANUAL, *supra* note 104, at 123.

118. Kerr, *supra* note 89, at 1228 (emphasis added).

119. *See* S. REP. NO. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N 3555, 3567. The 1968 definition of "contents" included "the identity of the parties or the existence of the communication. It thus distinguishes between the substance, purport, or meaning of that communication . . . ." *Id.*

from an account, and basic subscriber information would have all been considered noncontent in 1986.[120]

Case law interpreting the definition of "content" seems to turn on whether the user intended the communication.[121] In *In re Zynga Privacy Litigation*, the Ninth Circuit held "that under [the] ECPA, the term 'contents' refers to the *intended* message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication."[122] In reaching its decision, the court looked to the dictionary and noted that "(1) 'substance' means the characteristic and essential part, (2) 'purport' means the meaning conveyed, processed, or implied, and (3) 'meaning' refers to the thing one intends to convey . . . by language."[123] It further reasoned that these definitions indicated Congress's intent for the word "'contents' to mean a person's intended message to another (i.e., the 'essential part' of the communication, the 'meaning conveyed,' and the 'thing one intends to convey')."[124]

Additionally, in *In re iPhone Application Litigation*, the court held that because geolocation data were "generated automatically, rather than through the intent of the user . . . [they did] not constitute 'content' susceptible to interception."[125] Thus, in order to be considered content, the user himself must have intentionally generated the communication.

In its current form, the SCA provides almost no protection for individuals using wearables. The wearable serves as a platform to collect an abundant amount of information about the user, and the health app serves as a storage facility. Similar to location data, the user's health data are generated automatically—the user cannot simply choose to stop his heart rate.[126] Except in the circumstances where a user intentionally shares his health data with another user, his heart rate is a customer record. And even then, his shared heart rate may still be considered noncontent just like sharing location is considered noncontent. Although the SCA has potential to protect individual privacy for

120. *See* DOJ MANUAL, *supra* note 104, at 121. Basic subscriber information refers to "the identity of the subscriber, his relationship with his [ISP], and his basic session connection records." *Id.*

121. The case law in this area is scarce at best, but courts tend to view "intent" as the dispositive factor for contents of a communication. *See, e.g.*, *In re* Zynga Privacy Litig., 750 F.3d 1098, 1106 (9th Cir. 2014).

122. *Id.* (emphasis added). At issue in this case was whether Facebook violated the Wiretap Act by communicating users' identifying information to third party computers. When users would click on a gaming ad, Facebook would disclose to a third party both the user's Facebook ID and the webpage the user was viewing at the time he clicked the ad. The court ruled in favor of Facebook and held that this information was not the contents of a communication. *Id.* at 1099–103.

123. *Id.* (citations omitted) (internal quotation marks omitted).

124. *Id.*

125. 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012).

126. Critics have noted that the user could protect his privacy by removing the wearable altogether. Removing the device will not solve the overall problem, however, because of both the increasing number of wearables in the market and the unlikelihood that every user would cease using wearables completely. *See supra* note 43.

wearables, the content problem reveals why the SCA has not kept up with modern technology.

IV. PROPOSED SOLUTION: AMEND THE SCA TO INCLUDE "PERSONAL HEALTH DATA" IN ITS STATUTORY DEFINITION OF CONTENTS

Congress has the power to address the privacy concerns inherent in wearable devices. A weakness of the SCA is that it froze into law the understandings of technology as of 1986.[127] Relatively few people even had access to the Internet in 1986, yet now millions of individuals use the Internet on a daily basis.[128] This "increased personal use of the Internet to communicate and store communications . . . raise[s serious] questions about the adequacy of the privacy standards developed [by the SCA] . . . ."[129] Widespread personal use of e-mail, let alone wearable devices, was not in Congress's purview in 1986, yet the SCA appears to be the controlling statute in this realm.[130]

Simply put, the SCA does not adequately protect the privacy interests of individuals using wearables. According to the reasoning in *In re Zynga Privacy Litigation* and *In re iPhone Application Litigation*, most health data would not be considered content because they are generated automatically. Unlike the substantive portions of an e-mail, a person's health information is usually not intended (based on the common use of the word) to be a communication. Therefore, because health data likely do not receive the protections for content under section 2702(b), companies currently are completely free to disclose or sell customers' health data "to any person other than a governmental entity."[131]

In order to protect privacy for those who use wearables, Congress should amend the commercial component of the SCA to stipulate that health data are contents of communications when stored. To achieve this, Congress should append the following language to section 2510(8): "contents," when used with respect to any wire, oral, or electronic communication, includes (A) any information concerning the substance, purport, or meaning of that communication; and (B) for purposes of section 2702 of this title, includes any personal health data revealed in the communication.

For clarification, Congress should also add section 2510(22) to provide a new definition. It should state: "personal health data" mean any data of or relating to an individual's vital signs, physical health, or bodily details that would not be apparent to a degree of reasonable certainty through visual observation of the individual.

---

127. *See* Kerr, *supra* note 89, at 1214.

128. *See* Mulligan, *supra* note 77, at 1557.

129. *Id*. at 1558.

130. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 988 (C.D. Cal. 2010) (stating that the SCA is outdated and doesn't readily apply to modern communications).

131. 18 U.S.C. § 2702(c)(6) (2012).

The amendment would serve as a fair compromise between innovation and individual privacy. For purposes of voluntary disclosure to third parties, personal health information communicated through a wearable would be considered content. Thus, this expanded definition would provide health data with the same privacy protections afforded to content under section 2702(b) and would avoid leaving the data susceptible to the almost limitless disclosure authorization for noncontent under section 2702(c)(6). Additionally, this amendment would not interfere with the governmental component of the ECPA, as the expansion would be restricted to section 2702.

The "visual observation" limitation would serve to draw a line between observable information, such as physical location, and unobservable personal health data.[132] Visually observable bodily details would include outward medical symptoms, such as bloodshot eyes, but would not include unobservable vital signs such as heart rate. If a wearable communicates aspects of health that cannot be determined by the naked eye, those aspects will be considered content of a communication. Health-app companies would still be able to collect these personal health data, but would now be limited in their ability to readily disclose the data to third parties. This amendment may make the potential goldmine of health data less valuable, but it would allow individuals to enjoy a little more privacy in their quest to monitor their own health.

CONCLUSION

Consumer wearables present a new way for individuals to communicate sensitive, personal information about themselves. These same devices also provide a new way for companies to collect intimate data about individuals. Old laws must adapt to modern times in the same way that old methods of communication evolved with technology. A relatively unknown loophole in section 2702(c)(6) of the SCA allows health apps to freely disclose its customers' sensitive health information. But are people comfortable with companies knowing how truly lazy they are? How stressed they get around the holiday season? How their heart rate skyrockets whenever they are around certain people? How well they sleep? If not, Congress should step in and stop this widespread disclosure before it becomes irreversible. Until congressional intervention occurs, consumer wearables will continue to provide the platform for companies to, quite literally, profit from our heartbeats.

132. *See, e.g.*, *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) (holding that geolocation is not content).