BEWARE OF WEARABLES: PROTECTING PRIVACY IN A DATA-COLLECTING WORLD

Jessica Kitain[·]

ABSTRACT

Wearable devices collect an unprecedented amount of information from the most private facet of our lives – our bodies. As the technology grows, so too do concerns about protecting the privacy of the massive amounts of data collected. This Note presents the existing regulatory framework protecting data privacy, reviews the role of regulatory agencies, and ultimately exposes the gap between the protection of certain types of sensitive data and the lack of protection for all other data collected from the body through wearable devices. The solution to fill the gap lies in using the privacy principles of notice, choice, and consent in the United States' self-regulating system. Incorporating these fundamental principles will raise the privacy bar through industry standards and protect against potential onerous consequences in a global industry with rapidly evolving regulation.

· J.D. Candidate, 2017, Drexel University Thomas R. Kline School of Law; Bachelors of Arts, Psychology, Binghamton University. I would like to thank Professor Odia Kagan for introducing me to the law in the cyber world and Professor Alex C. Geisinger for serving as a supportive mentor. I also would like to thank the *Drexel Law Review* Editorial Board and staff members for making this Note possible.

TABLE OF CONTENTS

INTRODUCTION

In today's technological world, data collection has become one of the fastest growing, most widespread activities. It spans every single industry and facet of everyday life. "Every day, we create 2.5 quintillion bytes of data—so much that 90% of the data in the world today has been created in the last two years alone."[1]

This data includes more than what we enter into our computers or smartphones—it also comes from sensors constantly collecting data

1. *What Is Big Data?*, IBM, https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html (last visited Sept. 14, 2016).

from your body within wearable technology, "a market that is expected to top thirty-four billion dollars by 2020."[2] Think Fitbit, Apple Watch, and Google Glasses—devices worn with the capability of collecting information beyond the basic purpose marketed. So what? Consumers want more technology; not only for the novelty, but also for the convenience that is changing the way we live in the world. Isn't better technology that collects more data and improves daily life a good thing? It is, but consumers and businesses should be aware of associated risks and search for solutions to minimize them.

The two issues with data collection are security and privacy. Security is the protection of data from theft by way of hackers, or even authorized users, stealing the information.[3] Privacy revolves around protecting collected data from misuse by ensuring that the data will only be used in the authorized manner.[4]

The United States currently protects security and privacy of certain types of information with a statutory framework. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") protects health information used for treatment,[5] the Gramm-Leach-Bliley Act protects types of financial information used by financial institutions,[6] and certain types of Personal Identifiable Information ("PII") is federally regulated.[7] But, what about all other types of data?

For all other kinds of data, the United States is starting to fill the statutory void by using regulatory agencies to protect the security and privacy of information. The Federal Trade Commission, Federal

---

2. Paul Lamkin, *Wearable Tech Market to be Worth $34 Billion By 2020*, FORBES (Feb. 17, 2016, 9:31 AM), http://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/#a6b294a3fe38.

3. *See* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION A GUIDE FOR BUSINESS 9 (2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf; *see also* Edward J. McAndrew, *The Data Security Imperative for Lawyers*, 32 DEL. LAW. 30, 31 (2014) (noting that data security breaches include "cyber espionage, digital theft of consumer data, money and intellectual property, lost devices exposing private information, and disruption or destruction of digital infrastructure").

4. *See* Alicia Shelton, *A Reasonable Expectation of Privacy Online: "Do Not Track" Legislation*, 45 U. BALT. L. F. 35, 42–43 (2014). Shaun Spencer brings light to the balancing between the tangible harms that data security protects against versus the intangible harms of compromising the privacy of data. Shaun B. Spencer, *Security vs. Privacy: Reframing the Debate*, 79 DENV. U. L. REV. 519, 520–21 (2002). Often the intangible harms of an invasion of privacy are cast in the shadow of regulations that aim to increase security. *Id.*

5. *HIPPA for Professionals*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/index.html (last visited Sept. 14, 2016).

6. *Gramm-Leach-Bliley Act*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Sept. 14, 2016).

7. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2014).

Communications Commission, and Securities and Exchange Commission have all recently released mandatory principles that apply to collected data.[8] Several states have also individually issued regulations that protect the security and privacy of data for their residents.[9] Specifically, California is on the forefront of data protection with regulations mimicking the European Union standards.[10]

Now that regulatory agencies set the bar for a minimum standard of required security and privacy measures, businesses face onerous consequences for noncompliance in the form of twenty-year consent orders, a few of which are presented in this Note.[11] While regulatory agencies and state laws set forth a basic framework for security and privacy, the privacy component basically only requires notice and consent.[12] Although notice and consent are paramount, the growing use of wearable technology and the unprecedented amount of data collected leads to an inevitable conclusion—as businesses are required to notify users of exactly what data is collected and how it is used, Americans will eventually seek more protection and control over the information collected from their bodies. This Note addresses the concern over protecting private information, offering self-regulation as a solution to raise the privacy bar though industry standards.

Under the existing framework, for example, as long as a business notifies its user that the geolocation of that user is shared with unidentified third parties and that user consents to that use, the business is in full compliance with existing regulatory standards;[13] there is no requirement for a business to allow a user to opt-out of this information-sharing where the information is not protected under a specific Act.[14]

Instead of waiting for government regulation to implement new protections or risking regulatory agencies' heavy handed interference in the future, the wearable technology industry should implement the foundational privacy principles of notice, choice, and con-

---

8. *See* discussion *infra* Part I.F.

9. Lori Chiu, *Drawing the Line Between Competing Interests: Strengthening Online Data Privacy Protection in an Increasingly Networked World*, 14 SAN DIEGO INT'L L.J. 281, 285–87 (2013).

10. *See* discussion *infra* Part I.E.

11. *See* discussion *infra* Part I.G.

12. *See generally Consumer Privacy*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/consumer-privacy (last visited Sept. 14, 2016).

13. Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61, 117–18 (2011).

14. *See* King, *supra* note 13, at 116; *see also* Andrew J. McClurg, *A Thousand Words Are Worth A Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 133 (2003).

sent. These three foundational principles would raise the privacy standard, resulting in an industry where protecting private data is used as a business strategy to attract consumers mindful of data privacy while simultaneously future-proofing for evolving regulation in an expanding global market.

I. BACKGROUND

Wearable technology brings every day accessories to life, giving watches and glasses the capabilities to collect information directly from our bodies. In today's global market, it is crucial to explore all possible authorities governing the data collected. First, the U.S. sector-based approach is explored, as specific statutes regulate data based on the type of information. The U.S. sector-based regulation maintains strict protections of specific types of data as if privacy was a fundamental right. Next, the Note outlines the European Union approach to privacy as a fundamental right for all personal data. This section introduces the existing European framework and how the United States has attempted to meet these standards through self-regulation. Next are the California laws relating to privacy, which take a similar approach as the European Union in that privacy is considered a fundamental right. After parsing through the current data privacy frameworks, the current role of U.S. regulatory agencies is introduced to shed light on how the U.S. is attempting to regulate the massive amounts of consumer data that is otherwise not covered under the sector-based approach. Interference by regulatory agencies has resulted in onerous consequences for businesses found not in compliance with fair business practices regarding data, as seen in the form of strict and long-lasting consent orders.[15]

A. Wearable Technology: the Basics

Wearable technology is any device worn on the body that is equipped with sensors to collect information from both the body and the surrounding environment.[16] Wearable technology has the ability to transmit that information through the Internet.[17] Experts

15. *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

16. Dan Sung, *What Is Wearable Tech? Everything You Need to Know Explained*, WAREABLE (Aug. 3, 2015), http://www.wareable.com/wearable-tech/what-is-wearable-tech-753.

17. *Id.*

predict that the wearable technology industry will eventually grow into a $1.6 trillion business, giving rise to exciting new developments, as well as uncharted data privacy concerns.[18]

Wearable technology takes many different forms, but each device shares the common function of collecting real-time information directly from the body and transferring that information through the Internet.[19] The technology spans across different categories, such as activity trackers, running watches, wearable cameras, smart glasses, smart trackers, smart watches, and even wearables specifically for kids.[20] In just one day, a person may wear four or five wearables that constantly collect data.

Activity trackers, like the popular brand Fitbit, track the number of steps a person takes, the distance traveled, the number of calories burned, and sleeping habits.[21] Running watches, such as Garmin's Forerunner, track a person's heart rate and GPS location.[22] Wearable cameras, like the GoPro, have built-in Wi-Fi and Bluetooth capabilities.[23] Smart glasses, most recently taking the form of virtual reality head sets, track eye movements and body motions in order to give the experience of being in a three-dimensional reality, all while connected to the Internet.[24] Smart trackers are Bluetooth-tracking devices marketed as small devices that can be used to track items people regularly lose, like a set of keys or a cell phone.[25] Smart watches, like the Apple Watch, act like a smart phone connected to your body, sending and receiving information in real time over the Internet.[26]

Wearable technology is also created specifically for children, like the VTech Kidizoom Smartwatch, which has similar information-

18. Jayson Derrick, *Morgan Stanley: Wearable Technology a Potential $1.6 Trillion Business*, YAHOO! FIN. (Nov. 20, 2014), http://finance.yahoo.com/news/morgan-stanley-wearable-technology-potential-131618384.html; *see* Janice Phaik Lin Goh, *Privacy, Security, and Wearable Technology*, LANDSLIDE, Nov./Dec. 2015, at 30 .

19. *See, e.g.*, Sung, *supra* note 16.

20. *See, e.g.*, *id.*; *see Smartest Watch for Kids Gets Even Smarter with VTech's Kidizoom Smartwatch DX*, VTECH (Aug. 17, 2015), http://www.multivu.com/players/English/7465352-vtech-kidizoom-smartwatch-dx/.

21. *Fitbit Flex*, FITBIT, https://www.fitbit.com/flex (last visited Sept. 14, 2016).

22. *Garmin Forerunner*, GARMIN, http://explore.garmin.com/en-US/forerunner/ (last visited Sept. 14, 2016).

23. *GoPro HERO Session*, GOPRO, https://shop.gopro.com/cameras/hero-session/CHDHS-102.html (last visited Sept. 14, 2016).

24. *See* Sophie Charara, *Explained: How Does VR Actually Work?*, WAREABLE (June 20, 2016), http://www.wareable.com/vr/how-does-vr-work-explained.

25. *See How It Works*, THE TILE APP, https://www.thetileapp.com/how-it-works (last visited Sept. 14, 2016).

26. *See Apple Watch*, APPLE, http://www.apple.com/watch/ (last visited Sept. 14, 2016).

collecting capabilities to wearable technology for adults.[27] Considering the existing regulation of data gathered from children,[28] wearable technology for kids raises a unique set of concerns beyond the scope of this Note.

The vast capabilities of wearables to stream private information directly from the body is as exciting as it is concerning, especially when considering the fate of the data collected. Both businesses and consumers will benefit from filling the data privacy gap because the majority of the data collected from wearables falls into the category of consumer information not strictly protected to maintain privacy.[29]

B. Existing U.S. Sector-Based Approach for Protected Information

1. Gramm-Leach-Bliley Act

Recognizing the need to protect financial information, Congress enacted the Gramm-Leach-Bliley Act in 1999 (GLBA).[30] This act regulates financial institutions by setting standards for the security and privacy of customers' "nonpublic information" (NPI).[31] The GLBA requires financial institutions to establish standards to protect three basic principles:

> 1) to insure the security and confidentiality of customer records and information;
> 2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> 3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[32]

A financial institution subject to regulation under the GLBA includes any business "significantly engaged" in "financial activities."[33] In order to qualify as a financial institution under the GLBA,

---

27. *See Smartest Watch for Kids Gets Even Smarter with VTech's Kidizoom Smartwatch DX*, *supra* note 20.

28. *See, e.g.*, Children's Online Privacy Protection Act § 15 U.S.C. 6501–08 (2013).

29. *See* Phaik Lin Goh, *supra* note 18, at 31.

30. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 501, 133 Stat. 1338, 1436–37 (1999).

31. 15 U.S.C. § 6801 (2011).

32. *Id.*

33. *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FED. TRADE COMMISSION 2 (July 2002) [hereinafter *GLBA FTC Compliance*], https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

two factors must be met: (1) the existence of a formal arrangement and (2) the business must regularly engage in financial activity.[34]

The protected NPI includes any information given to a financial institution to receive a financial product or service; any information gathered about an individual while providing a financial product or service; and any information collected about an individual from a transaction involving a financial product or service.[35] GLBA does not cover information that is "publicly available," such as an individual's telephone number that is already listed in a public phone book.[36]

The GLBA has two main components, the Safeguards Rule[37] and the Privacy Rule. [38] The Safeguards Rule requires that financial institutions maintain appropriate administrative, technical, and physical safeguards by creating an information security program.[39] The rule sets forth five elements that the program must contain in order to be in compliance with GLBA:

(1) designate an employee or employees to coordinate the information security plan; (2) identify reasonably foreseeable internal and external risks to the security; (3) design and implement information safeguards to control the risks identified; (4) oversee that service providers maintain safeguards; and (5) evaluate and adjust the information security program after regular testing and monitoring of the program.[40]

The Privacy Rule component of GLBA sets forth basic obligations founded in the principles of providing individuals with notice and receiving consent before using their NPI.[41] Generally, financial institutions may not disclose NPI to nonaffiliated third parties without providing the individual notice and the ability to opt out of such information sharing.[42] The Privacy Rule also requires financial institu-

34. *Id.* at 2–3.

35. *Id.* at 4–5.

36. *Id.* at 5.

37. 16 C.F.R. § 314.1 (2002); *Safeguards Rule*, FED. TRADE COMMISSION, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule (last visited Sept. 14, 2016).

38. 15 U.S.C. § 6801 (2011); *GLBA FTC Compliance*, *supra* note 33, at 2.

39. 16 C.F.R. § 314 (2002).

40. 16 C.F.R. § 314.4 (2002).

41. 15 U.S.C. § 6801; *see generally GLBA FTC Compliance*, *supra* note 33, at 6–11 (providing an overview of obligations under GLBA's Privacy Rule).

42. 15 U.S.C. § 6801; *GLBA FTC Compliance*, *supra* note 33, at 6–7.

tions to disclose all uses of NPI and to include specific information in the disclosures.[43]

2. Health and Insurance Portability and Accountability Act

In recognition of the need to protect sensitive medical information, Congress passed the Health Insurance Portability and Accountability Act in 1996 (HIPAA). The purpose of HIPAA is to establish standards for electronically transmitting health information for the use of treating patients.[44]

HIPAA only applies to covered entities and business associates, and it only safeguards Protected Health Information (PHI).[45] A covered entity (CE) is a health care provider, a health plan, or a health clearinghouse.[46] A business associate (BA) engages with a CE to carry out health care functions and activities.[47]

PHI protected by HIPAA is individually identifiable health information that is either transmitted or maintained by a CE or BA.[48] Individually identifiable health information includes demographic information, information relating to an individual's mental or physical health, information regarding the provision and payment of health care, and information identifying the individual.[49]

Like GLBA, HIPAA also has a Security Rule[50] and a Privacy Rule.[51] The Security Rule requires CEs and BAs to maintain appropriate administrative, technical, and physical safeguards for protecting PHI by:

> 1) Ensur[ing] the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;

---

43. *GLBA FTC Compliance*, *supra* note 33, at 7–8.

44. 45 C.F.R. § 163.502 (2013); *Why is the HIPPA Privacy Rule Needed?*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES (Nov. 9, 2011), http://www.hhs.gov/hipaa/for-professionals/faq/188/why-is-the-privacy-rule-needed/index.html.

45. *Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Sept. 14, 2016).

46. *Id.*

47. *See id.*

48. 45 C.F.R. § 160.103 (2013).

49. *Id.*

50. *Summary of the HIPAA Security Rule*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Sept. 14, 2016) [hereinafter *HIPAA Security Rule*].

51. *Summary of the HIPAA Privacy Rule*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/ (last visited Sept. 14, 2016) [hereinafter *HIPAA Privacy Rule*].

> 2) Identify[ing] and protect against reasonably anticipated threats to the security or integrity of the information;
> 3) Protect[ing] against reasonably anticipated, impermissible uses or disclosures; and
> 4) Ensure compliance by their workforce.[52]

The Privacy Rule specifies how protected health information may be used and disclosed by identifying "permitted" uses and disclosures and "authorized" uses and disclosures.[53] The rule also establishes the "minimum necessary" principle, requiring CEs to only collect the minimum amount of PHI necessary to carry out the information's intended purpose.[54] It is also required that CEs notify individuals of the privacy policy and gain authorization for any use of the PHI.[55]

3. Children's Online Privacy Act

Consistent with the view of protecting children as a vulnerable population, Congress enacted the Children's Online Privacy Protection Act ("COPPA") in 1998.[56] COPPA gives parents control over what information is collected from their children on the Internet by requiring websites that target children to receive parental consent before collecting certain types of information from children.[57] COPPA also completely forbids the collection of certain types of information from children.[58]

Under COPPA, any website either directed at children or knowingly collecting personal information from children must: (1) "provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information"; and (2) "obtain verifiable parental consent for the collection, use, or disclosure of personal information from children."[59] Further, at the parent's request, a website must describe what type of personal information was collected from the child, give that parent the opportuni-

---

52. *HIPAA Security Rule*, *supra* note 50.

53. *HIPAA Privacy Rule*, *supra* note 51.

54. *Id.*

55. *Id.*

56. *See Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMMISSION (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions.

57. 15 U.S.C. § 6502(b)(1) (1998).

58. *Id.*

59. 15 U.S.C. § 6502(b)(1)(A)(i)–(ii).

ty to refuse to allow the website to further use the information collected, and give the parent access to the information collected from the child.[60]

Beyond giving parents control and access to the information collected from their children, COPPA prohibits websites from requiring disclosure of "more personal information than is reasonably necessary" from a child as a condition for that "child's participation in a game, [receiving] a prize, or another activity."[61] COPPA also includes a general provision requiring websites that collect personal information from children to "maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[62]

4. Family Educational Rights and Privacy Act

In furthering the protection of children and their personal information, the Family Educational Rights and Privacy Act of 1974 ("FERPA") includes the protection of the privacy of student's educational records.[63] While the privacy protections surrounding FERPA began before cyber data privacy and security issues existed, electronic student records today elicit the same privacy and security concerns as other forms of electronic information viewed as needing regulation.

FERPA affects any school that receives federal funding from the U.S. Department of Education.[64] The federal law gives parents of students under the age of 18 attending these schools the right to inspect and review the student's records maintained by the school and to request that the school correct any inaccurate information.[65] Schools are also prohibited from releasing any student's educational records without consent of the parent, although there are certain entities that may receive student educational records from a school without consent.[66]

---

60. 15 U.S.C. § 6502(b)(1)(B)(i)–(iii).

61. 15 U.S.C. § 6502(b)(1)(C).

62. 15 U.S.C. § 6502(b)(1)(D).

63. *Family Educational Rights and Privacy Act (FERPA)*, N.Y. UNIV. (Jan. 1, 2009), http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/FERPA.html.

64. *Family Educational Rights and Privacy Act (FERPA)*, U.S. DEP'T OF EDUC. (June 26, 2015), http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

65. *Id.*

66. *Id.*

C. European Union: Protecting Data Privacy as a Fundamental Right

The legal framework of the European Union ("EU") is drastically different from the sector-based approach taken in the United States; under the EU framework, privacy is a fundamental right.[67] Under this framework, collecting personal data from an EU citizen must comply with strict legal conditions, and the information can only be gathered for a legitimate purpose.[68] Approaching data privacy as a fundamental right put the EU on the forefront of data privacy[69] and most recently exposed the U.S. to serious penalties for not complying with its approved regulations.[70]

The EU data privacy regulations are important for U.S. companies for two reasons. First, any U.S. company that collects information in the EU is subject to EU law.[71] Second, and less obvious, is the idea that the EU framework should motivate U.S. companies in the wearable technology industry to achieve the same data privacy protections afforded by the EU framework through self-regulation of the industry.

The EU first enacted the Directive on Data Protection ("1995 Directive") in 1995, subsequently updating it over time as technology evolved.[72] The purpose of the 1995 Directive is to create a safe and

---

67. *Compare Information Society, Privacy and Data Protection*, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection (last visited Sept. 14, 2016) *with* CHRIS HOOFNAGLE, EUROPEAN COMM'N, COMPARATIVE STUDY ON DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS: B.1—UNITED STATES OF AMERICA (2010), http://webcache.googleusercontent.com/search?q=cache:ErkKSJE2IukJ:ec.europa.eu/justice/dataprotetion/document/studies/files/new_privacy_challenges/final_report_country_report_b1_usa.pdf+&cd=1&hl=en&ct=clnk&gl=us

68. *Protection of Personal Data*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/ (last updated Feb. 8, 2016).

69. *See* EUROPEAN DATA PROT. SUPERVISOR, ANNUAL REPORT 2015 5, 7 (2016), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2015/EDPS_Annual_Report_2015_Web_EN.pdf.

70. *See* Scott Vernick & Jessica Kitain, *The Right to Be Forgotten—Protection or Hegemony?*, BLOOMBERG BNA: WORLD DATA PROTECTION REPORT (June 28, 2016) (discussing the legal battle between Google and Spain over EU data regulation, which conflicts with the U.S. approach).

71. European Commission Press Release IP/15/6321, Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market (Dec. 15, 2015), http://europa.eu/rapid/press-release_IP-15-6321_en.htm [hereinafter EU Data Protection Reform].

72. *Welcome to the U.S.-EU Safe Harbor*, EXPORT.GOV, https://build.export.gov/main/safeharbor/eu/eg_main_018365 (last updated July 26, 2016, 12:38 PM).

secure cyber network between the member states while upholding privacy, an EU core value, as a human right.[73] While EU law does not bind the U.S.,[74] the Internet is a global platform, and the EU holds any company that collects information from EU citizens to standards of the 1995 Directive.[75]

On December 15, 2015, the European Parliament and Counsel agreed to implement stricter data privacy and security regulation than the regulations in the 1995 Directive,[76] most notably agreeing to give data protection authorities the ability to fine companies not in compliance with the regulations "up to 4% of their global annual turnover."[77] The possibility of such a substantial fine is a new reality for huge companies that regularly collect data from EU citizens, including companies like Amazon, Apple, Google, and Facebook.[78]

The EU reformed the 1995 Directive into two distinct frameworks: 1) the General Data Protection Regulation ("Regulation"), which sets forth protections for personal data processed by the private sector; and 2) the Directive on the Processing of Personal Data for Law Enforcement ("Directive"), which sets forth protections for personal data processed by authorities in connection with a criminal offense or investigation.[79] The EU adopted the reformed Regulation and the reformed Directive in April 2016.[80] The Regulation, the relevant framework to privacy of personal data in the private sector, entered into force on May 24, 2016.[81]

The Regulation improves and refines the 1995 Directive in six major ways.[82] First, the Regulation requires that a person must give

---

73. *EU Cyber Security Strategy – Open, Safe and Secure*, EUROPEAN UNION (July 2, 2013), http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm.

74. Gráinne de Búrca, *International Law Before the Courts: the EU and the US Compared*, 55:3 VA. J. OF INT'L L. 685, 699–700 (2015).

75. *Welcome to the U.S.-EU Safe Harbor*, *supra* note 72.

76. EU Data Protection Reform, *supra* note 71.

77. European Commission Fact Sheet MEMO/15/6385, Questions and Answers - Data Protection Reform (Dec. 21, 2015), http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm [hereinafter Q&A Data Protection Reform].

78. Kelly Couturier, *How Europe Is Going After Google, Amazon and Other U.S. Tech Giants*, N.Y. TIMES, http://www.nytimes.com/interactive/2015/04/13/technology/How-Europe-Is-Going-After-U.S.-Tech-Giants.html (last updated Aug. 30, 2016).

79. Vernick & Kitain, *supra* note 70.

80. *Reform of EU Data Protection Rules*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last updated Feb. 8, 2016).

81. *Id.*

82. *See* Vêra Jourová, *How Does the Data Protection Reform Strengthen Citizens' Rights?*, EUROPEAN COMMISSION 1–2 (Jan. 2016),

clear and affirmative consent before a company can process that person's personal data.[83] Second, the Regulation strengthens the "right to be forgotten, which means that if you no longer want your personal data to be processed, and there is no legitimate reason for a company to keep it, the data shall be deleted."[84] Third, the Regulation guarantees that people have free and easy access to their personal data.[85] Fourth, the Regulation improves data portability by making it easier for people to have their data transferred between service providers.[86] Fifth, the Regulation imposes a mandatory breach notification period of 72 hours.[87] Lastly, the Reform sets forth the principle of "data protection by design."[88] This principle requires data protection as a default in the development stage of products and services that use and collect personal data.[89]

D. European Union: Safe-Harbor as a Model for Data Protection

The Safe-Harbor Framework was created in response to the 1995 Directive, prohibiting data transfer to non-EU member countries that do not follow the EU "adequacy" standard in order to maintain and encourage an international flow of information.[90] Safe-harbor is a self-regulating certification that a company displays on its website to ensure that the company protects data to the standard set forth by the EU for non-EU countries collecting this information from EU citizens.[91]

Although the EU adopted the Safe-Harbor Framework as "adequate" data protection in 2000, the ruling in *Schrems v. Data Protection Commissioner* invalidated the Safe-Harbor Framework as not satisfying the "adequate protection" requirement.[92] Despite this ruling,

---

http://ec.europa.eu/justice/dataprotection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf.

83. *Id.* at 1.

84. *Id.*

85. *Id.* at 2.

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. *Welcome to the U.S.-EU Safe Harbor*, *supra* note 74.

91. *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, https://build.export.gov/main/safeharbor/eu/eg_main_018476 (last updated Dec. 18, 2013).

92. *See Max Schrems v. Irish Data Protection Commissioner (Safe Harbor)*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/intl/schrems/ (last visited Aug. 5, 2016). In the case, the plaintiff, an EU citizen, claimed that the U.S. laws and practices allowing the NSA access to in-

the Safe-Harbor Framework offers valuable guidance for wearable technology companies that easily and effectively increases the protection of private data.[93]

The Framework consists of seven privacy principles that a company must meet in order to be Safe-Harbor certified: (1) Notice; (2) Choice; (3) Onward Transfer (Transfers to Third Parties); (4) Access; (5) Security; (6) Data Integrity; and (7) Enforcement.[94] The first two principles, notice and choice, offer the most guidance for ensuring that a strong foundation will be implemented in protecting the privacy of data.[95]

To satisfy the notice requirement, companies are required to inform consumers of the purpose of collecting the data and how that information will be used.[96] Companies must also notify a consumer with whom the consumer's information is shared as well as what choices are available in terms of limiting the uses of the data.[97] Lastly, companies must provide consumers with their contact information for any questions or complaints that arise.[98]

To satisfy choice, companies must give consumers the choice to opt out of sharing their personal information with third parties for a purpose other than for what the information was originally collected.[99] If data is considered sensitive information, consumers must be given an affirmative opt-in choice to limit information sharing with third parties for a purpose other than the originally intended purpose, or a purpose subsequently authorized by the consumer.[100]

The Safe-Harbor approach to notice, choice, and consent offers an easy and effective method for promoting data privacy. Implementing these principles gives consumers knowledge and control over private information.

---

formation from Facebook does not offer real protection against surveillance by the U.S., thereby violating the privacy of E.U. citizens, and the court subsequently agreed. *Id.*

93. *U.S.-EU Safe-Harbor Overview*, *supra* note 91.

94. *Id.*

95. *See id.*

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.*

E. California Privacy Laws

Similar to the EU's view, the state of California classifies privacy as a fundamental right.[101] With the framework of viewing privacy as a fundamental right, California is on the forefront of U.S. data privacy.[102] California enacted legislation that institutes higher standards of protection for each sector of information currently protected by federal law.[103] Furthermore, California's online privacy regulations reach further than any other state, most notably with the Online Privacy Protection Act of 2003.[104] It is crucial to consider California's privacy regulations in terms of wearables, as the technology inevitably reaches California residents, triggering enforcement of the state-specific laws.

The Online Privacy Protection Act of 2003 requires that all operators of commercial websites post a privacy policy on its website, and the Act specifically details what the policy must contain.[105] First, the policy must identify all categories of personally identifiable information collected and with whom that information is shared.[106] If there is a process that allows the consumer to access his or her information, the policy must explain that process.[107] Next, the policy must inform the consumer how he or she will be notified if there are any changes to the privacy policy and identify the effective date of the policy.[108] The policy must also inform the consumer of choice options, and whether third parties can collect information about the consumer's online activities over time.[109]

F. Protecting Consumer Data in the U.S.

Most data collected by wearable technology does not satisfy the statutory requirements under an existing federal Act. Therefore, all of the data collected by wearable technology inevitably falls under

---

101. *See* CAL. CONST. art. 1, § 1.

102. *See* California Electronic Communications Privacy Act, ch. 651 Cal S.B. 178 (requiring state law enforcement to get a warrant before they can access certain electronic information); *see* Warwick Ashford, *California adopts landmark law protecting digital privacy*, COMPUTERWEEKLY.COM (Oct. 9, 2015), http://www.computerweekly.com/news/4500255186/California-adopts-landmark-law-protecting-digital-privacy.

103. Ashford, *supra* note 102.

104. *See* CAL. BUS. & PROF. CODE § 22575 (West 2004).

105. *Id.* § 22575(a)–(b).

106. *Id.* § 22575(b).

107. *Id.*

108. *Id.*

109. *Id.*

the broad category of consumer data, triggering the oversight of regulatory agencies protecting consumers: the Federal Trade Commission, the Federal Communications Commission, and the Securities and Exchanges Commission.

1. Federal Trade Commission

The Federal Trade Commission ("FTC") is authorized, by the FTC Act § 45, to enforce cease-and-desist orders against any entity found to have "unfair or deceptive acts or practices" involving the management of data.[110] This governmental agency is the leading force behind the current crusade against poor data protection. The basic framework for identifying unfair acts or practices consists of analyzing whether the business act "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[111] A business engages in deceptive acts or practices when "a representation, omission, or practice . . . is *likely* to mislead the consumer acting *reasonably* in the circumstances, to the consumer's *detriment*."[112]

In May, 2000, the FTC released a report to Congress, *Fair Information Practices in the Electronic Marketplace*, outlining three basic privacy principles that should guide business' privacy practices: (1) Notice; (2) Choice; and (3) Access.[113] Notice refers to providing consumers with "clear and conspicuous notice of their information practices."[114] The guide specifically outlines how information is collected, how it is used, and with whom the information is shared.[115] Choice refers to giving consumers the option to decide how their information is used beyond the use for which it was originally provided.[116] This choice involves giving consumers the options of how the information is used internally, such as for marketing back to the

110. Federal Trade Commission Act, 15 U.S.C. § 45(b) (2006).

111. 15 U.S.C. § 45(n).

112. Sw. Sunsites, Inc. v. F.T.C., 785 F.2d 1431, 1435 (9th Cir. 1986).

113. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE i, iii (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf (outlining not only the three described principles, but a fourth principle, security, requiring businesses to take "reasonable steps" to protect information they collect).

114. *Id.* at iii.

115. *Id.*

116. *Id.*

consumer, and externally, such as disclosing the information to third parties.[117] Lastly, access refers to giving consumers reasonable access to the information collected about them, including "a reasonable opportunity to review information and to correct inaccuracies or delete information."[118]

In practice, these standards manifest in a "we know it when we see it" method, as seen in the recent Third Circuit decision, *FTC v. Wyndham Worldwide Corp.*, where the court found that Wyndham Hotel engaged in business practices rising to the level of unfair and deceitful.[119] The biggest problem with the opinion from *FTC v. Wyndham Corp*. is that the court failed to set forth more clearly defined standards, as the facts in the case indicated clear evidence of unfair and deceitful business practices.[120]

Although the decision in *FTC v. Wyndham Worldwide Corp.* did not set forth clearly defined data security and privacy standards, it solidified the FTC's authority to regulate and enforce consent orders against businesses that partake in unfair and deceptive business practices in terms of cybersecurity.[121]

In response to the uncertainty surrounding the *FTC v. Wyndham Worldwide Corp.* ruling, the FTC released a guide for businesses in an attempt to compile more concise security guidelines for businesses to implement to avoid FTC enforcement.[122] It is crucial to note that the guideline is for security, and the FTC approach to consumer privacy offers much less guidance.

In terms of the information regulated by the FTC that is not covered under a specific statutory framework, the approach to protection is extremely basic. The FTC released reports on balancing privacy and innovation,[123] giving consumers a choice,[124] and properly

---

117. *Id.*

118. *Id.*

119. 799 F.3d 236, 249 (3rd Cir. 2015). Plaintiff is a hotel and resort chain that maintained virtually no cybersecurity procedures, resulting in three security breaches affecting approximately 619,000 consumers and resulted in a loss of over $10.6 million in fraudulent charges. *Id.* at 240–42. The court found that the lack of password protection and encryption, despite the company's claim to cybersecurity, rose to unfair and deceitful business practices. *Id.* at 248.

120. *Id.*

121. *Id.* at 248.

122. FED. TRADE COMM'N, LESSONS LEARNED FROM FTC CASES (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

123. *See generally FTC's Privacy Report: Balancing Privacy and Innovation*, FED. TRADE COMMISSION (Mar. 2012), https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report.

124. *See generally The Do Not Track Option: Giving Consumers a Choice*, FED. TRADE COMMISSION (2010), https://www.ftc.gov/news-events/media-resources/protecting-consumer

notifying consumers as to what is being done with their information.[125] These reports are purely recommendations; there is no legal framework, beyond unfair and deceptive business practices, to hold businesses accountable in terms of privacy of information not deemed protected under a statutory framework.

2. Federal Communications Commission

The Federal Communications Commission ("FCC") is also getting involved in promoting data security and privacy. The FCC entered the world of cybersecurity after issuing a $10,000,000 fine against two telecommunications companies that engaged in negligent business practices putting about 300,000 customers at risk.[126] In terms of security guidelines, the FCC has released security tips for small businesses,[127] released a cybersecurity risk management and best practices guide,[128] and asked for public input on that guide.[129]

In terms of privacy, the FCC released a public notice in May 2015 that the agency will enforce 47 U.S.C. § 222, Privacy of Customer Information on all broadband providers.[130] The FCC will determine if

---

-privacy/do-not-track.

125. *See generally Making Sure Companies Keep their Privacy Promises to Consumers*, FED. TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting -consumer-privacy/enforcing-privacy-promises (last visited Aug. 23, 2016).

126. Tom Risen, *FCC Adds Cybersecurity to its Oversight*, U.S. NEWS (Oct. 24, 2014, 5:06 PM), http://www.usnews.com/news/articles/2014/10/24/fcc-adds-cybersecurity-to-its -oversight. Companies YourTel America and TerraCom Inc. used sensitive consumer information to determine who qualified for the low-income cellphone program (Obamaphone) without encrypting any of the data. *Id.* The sensitive data included social security numbers, addresses, names, and driver's license information. *Id.* The FCC found that both companies breached "the privacy and trust of their customers" and subsequently issued a $10 million fine. *Id.*

127. FED. COMMC'NS COMM'N, TEN CYBERSECURITY TIPS FOR SMALL BUSINESSES, https://apps.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf (last visited Sept. 9, 2016).

128. THE COMMUNICATIONS SECURITY, RELIABILITY AND INTEROPERABILITY COUNSEL, CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES WORKING GROUP 4: FINAL REPORT (Mar. 2015), http://www.hldataprotection.com/files/2015/04/CSRIC_WG4_Report_Final_March_18_201 5.pdf.

129. Mark Brennan and Paul Otto, *FCC Seeks Comment on Cybersecurity Recommendations for Communications Providers*, HOGAN LOVELLS (Apr. 23, 2015), http://www.hldataprotection.com/2015/04/articles/cybersecurity-data-breaches/fcc-seeks -comment-on-cybersecurity-recommendations-for-communications-providers/.

130. FED. COMMC'NS COMM'N, ENFORCEMENT BUREAU GUIDANCE: BROADBAND PROVIDERS SHOULD TAKE REASONABLE, GOOD FAITH STEPS TO PROTECT CONSUMER PRIVACY 1 (May 20, 2015), http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0520/DA-15 -603A1.pdf.

broadband providers are taking "reasonable, good-faith steps to comply with Section 222."[131] Section 222(a) states that broadband providers are prohibited from using "proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers" for its own marketing purposes.[132]

A legal standard of reasonableness and good faith is not a workable framework for businesses to follow. Further, the limited scope of the regulation leaves open the possibility of many other uses of the information, as the information is not directly protected under a different statutory framework.

3. Securities and Exchange Commission

The Security and Exchange Commission ("SEC") joined the push for data security by enforcing the Safeguards Rule and issuing guidance on best security practices.[133] In September 2015, the SEC settled charges against a St. Louis investment advisor for failing to establish the required cybersecurity policies required under the Safeguard Rule.[134] In terms of privacy, the SEC is concerned with mostly financial information, which falls under the GLBA framework, therefore the SEC has not issued independent guidance on privacy.[135]

G. Existing Consequences for a Failure to Protect Data: FTC Consent Orders

The FTC enforcement against unfair or deceptive business practices is seen in action through the existing consent orders issued against companies that violate the data privacy and security of their consumers. Three existing consent orders shed light on acceptable standards, the onerous consequences that may result from a business failing to protect consumers' data privacy, and the growing need to guard against inevitable concerns regarding the protection of the privacy of data collected from wearables.

---

131. *Id.* at 2.

132. 47 U.S.C. § 222(a) (2008).

133. *See* 16 C.F.R. § 314.4 (2002).

134. *SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach*, U.S. SEC. & EXCHANGE COMM. (Sept. 22, 2015), http://www.sec.gov/news/pressrelease/2015-202.html.

135. *See generally* 16 C.F.R. § 314.1 (2002) (noting its application to financial institutions).

1. Google

In October 2011, the FTC served a consent order on Google and subsequently filed a complaint against Google for partaking in unfair and deceptive business practices.[136] Although Google represented to its users that it would not place tracking "cookies" or serve targeted ads based on those tracking cookies, Google subsequently did just that.[137] The information Google provided to its users was not only deceptive and misleading, but also a blatant misrepresentation of how users' information was being used.[138]

The consent order, in effect for 20 years, sets forth a detailed plan with strict compliance deadlines.[139] The consent order is broken down into nine parts, each directing Google to comply with mandatory guidelines.[140] Parts I, II, and III are most relevant to privacy by instituting mandatory requirements under the close watch of the FTC.[141]

Part I forbids Google from misrepresenting in any manner the extent to which it "maintains and protects the privacy and confidentiality of any covered information."[142] This includes any misrepresentation as to the purpose for collecting and using the information as well as the extent to which the individual has control over the information provided.[143]

Part II instructs Google to "[o]btain express affirmative consent" from users before sharing covered information in a way that is dif-

136. United States v. Google Inc., No. CV 12-04177 SI, 2012 WL 5833994, at *1, *2 (N.D. Cal. Nov. 16, 2012); *In re* Google, Inc., F.T.C. File No. 102 3136 (2011) [hereinafter Google Consent Order], https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf.

137. *Google*, 2012 WL 5833994, at *1; *see also Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Brower*, FED. TRADE COMMISSION (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

138. *See Google*, 2012 WL 5833994, at *1. Google sold users' information to advertisers to deliver targeted advertisements to those users, and in 2011, received $36.5 billion from advertising fees, approximately $1.7 billion coming from online display ads. Complaint at 4, United States v. Google Inc., No. CV 12-04177 (Aug. 8, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf.

139. Google Consent Order, *supra* note 136 at 7.

140. *Id.* at 3–9.

141. *Id.* at 3–5.

142. *Id.* at 4. "[C]overed information" is defined in the consent order as pertaining to any information collected from an individual user. *Id.* at 3.

143. *Id.* at 4.

ferent from what was originally agreed upon, whether in the "terms of use" or "privacy policy."[144]

Part III creates a mandatory obligation to institute a "comprehensive privacy program" in order to assess privacy risks and protect the privacy of the existing covered information.[145] This section also outlines the necessary components of the comprehensive privacy program, including designating a specific employee or employees to be responsible for the program, assessing and managing privacy risks, creating privacy control procedures, managing service providers that deal with the covered information, and constantly evaluating, monitoring, and testing the program.[146]

2. Nomi Technologies

Nomi Technologies provides retailers with information about shoppers in their stores who use a "mobile device tracking technology."[147] Nomi's service, "Listen," installs sensors in participating retail stores that identify mobile devices by picking up a unique 12-digit identifier—media access control "MAC" address—which is emitted from cell phones searching for available Wi-Fi networks.[148] In other words, Listen picks up a signal from each cell phone that enters a retail store where Listen is installed, and the signal is unique to that specific cell phone. Although seemingly innovative and beneficial for businesses, Nomi failed to provide consumers with a list of participating retailers and did not require retailers to disclose the presence of Listen in their stores.[149] Further, Nomi posted a privacy policy on its website that offered consumers an "opt out" to Listen.[150] It required consumers to enter in their MAC address on Nomi's website, despite not knowing the identity of participating retailers.[151] Furthermore, consumers were not given the option to opt out of Listen at specific retailers' locations.[152]

144. *Id.*

145. *Id.*

146. *Id.* at 4–5.

147. Complaint at 1, *In re* Nomi Techs., F.T.C. File No. 132 3251 (Aug. 28, 2015) (No. C-4538), https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf.

148. *Id.*

149. *Id.* at 2.

150. *Id.*

151. *Id.* at 3.

152. *Id.*

In addition to filing a complaint, the FTC issued a six-part consent order against Nomi Technologies for misleading consumers.[153] Part I expressly forbids Nomi from misleading consumers about the options to control their information and the extent to which their information is shared.[154] Parts II–VI focus on mandatory administrative duties, such as maintaining records of compliance at all times for FTC inspection, notifying the FTC of any changes in the corporation, filing a mandatory initial report with the FTC, and continuing compliance with the consent order for twenty years.[155] Additionally, Nomi will be responsible for providing all employees and individuals involved in the company with a copy of the consent order for ten years.[156]

3. Trendnet Inc.

Trendnet Inc. is a company that provides cameras for security purposes, such as home monitoring or watching children with a babysitter.[157] The cameras' live feed is accessible through the consumer's computer or mobile phone.[158] Access to a camera requires a login and password, but also has a setting to disable the password protection in order to access the feed.[159]

Trendnet further purported the security of its product by using the trade name "Securview" on the cameras' packaging, on its website, and on its app.[160] A sticker with a picture of a lock and the word "Security" was also found on the packaging.[161] Although claiming that the camera was a security feature for the home, Trendnet's unfair business practices surrounding the actual security measures placed consumers at significant risk.[162]

Despite its marketing, Trendnet failed to institute even the most basic security measures in terms of its software. Trendnet stored and transmitted user login credentials in plain, readable text and failed

153. *In re* Nomi Techs., Inc., F.T.C. File No. 132 3251 (Aug. 28, 2015) (No. C-4538) [hereinafter Nomi Consent Order], https://www.ftc.gov/system/files/documents/cases/150902nomitechdo.pdf.

154. *Id.* at 2.

155. *Id.* at 2–3.

156. *Id.* at 3.

157. Complaint at 2, *In re* Trendnet Inc., F.T.C. File No. 122 3090 (Jan. 16, 2014) (No. C-44), https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

158. *Id.*

159. *Id.*

160. *Id.* at 3.

161. *Id.*

162. *Id.* at 5.

to secure the data that allowed access to live feed video in users' homes.[163] Besides the potential risks to consumers, hackers were able to access the cameras and post a live feed of approximately 700 users' cameras.[164] The FTC determined that Trendnet violated the most basic security measures necessary, and therefore instituted a consent order detailing strict security requirements.[165]

Part I of the consent order forbids Trendnet from misleading consumers as to its security measures or to the extent a consumer has control over the covered information.[166] Part II requires Trendnet to institute a security program in order to (1) address security risks and (2) protect the security of the data collected.[167] This part maps out a detailed plan for the security program in order to assure that the risks are properly assessed, all service providers are monitored, and the program itself is monitored and adjusted as risks develop.[168]

Part III requires Trendnet to complete an initial assessment followed by assessments every other year, which must be completed by an objective third party professional.[169] The assessment must review Trendnet's progress of compliance with the required security program and must certify that the security program is operating in a manner that is "sufficiently effective."[170]

Part IV requires Trendnet to notify all affected consumers that the camera was flawed because it allowed third parties to access a live feed through the camera without the consumer knowing.[171] This part sets forth strict timelines for notifying affected consumers and also requires Trendnet to clearly and easily offer "prompt and free support" to help consumers uninstall their camera.[172]

Parts V–IX set mandatory administrative requirements for Trendnet to continue to provide and maintain information to the FTC.[173]

---

163. *Id.* at 4.

164. *Id.* at 5.

165. *In re* Trendnet, Inc., F.T.C. File No. 122 3090 at 4 (Jan. 16, 2014) [hereinafter Trendnet Consent Order], https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf; *see, e.g.*, *Webcam Maker Takes FTC's Heat For Internet-of-Things Security Failure*, TECHNEWSWORLD, http://www.technewsworld.com/story/78891.html (last visited Aug. 12, 2016) (calling Trendnet's security "laxed").

166. Trendnet Consent Order, *supra* note 165 at 4.

167. *Id.* at 5.

168. *Id.*

169. *Id.* at 6.

170. *Id.*

171. *Id.* at 7.

172. *Id.*

173. *Id.* at 7–9.

All employees and individuals involved with the company's operations must be notified and all records must be maintained.[174] Additionally, the consent order is to remain in effect for twenty years.[175]

Each consent order discussed exposes the heavy hand of regulatory agencies. These consent orders also illustrate the importance of notice, choice, and consent. These basic principles hold a place in the mandatory procedures that must be put in place and monitored for twenty years.

II. ANALYSIS

While the capabilities of wearable technology are unprecedented, there is a growing concern in the legal community as to the security and privacy implications arising from the massive amounts of data collected.[176] Security of the data collected from wearables depends on a company having the proper technological and procedural safeguards in place as well as a response plan in the event of a breach. The more pressing concern is the issue of privacy, as the data collected from the wearable technology is not specifically protected under the current U.S. sector based framework.[177] Self-regulation is the solution to fill the gap in protecting the privacy of data.

The massive amounts of data collected by wearable technology raises an instinctual concern for the need to protect the type of information collected from an individual's body. Wearable technology's ability to collect the most private information is alarming; over the course of a single day, a wearable can record an individual's heart rate, calculate the number of steps the individual took, and even record where those steps were taken, down to specific rooms in a house or building.[178] If this type of information found its way into the wrong hands, consequences could be extremely destructive. An individual consenting to a wearable device collecting such private information would certainly think twice if such information

---

174. *Id.* at 8.

175. *Id.* at 9.

176. Zainab Hussain, *Weary of Wearables: IP, Privacy, and Data Security Concerns*, LAW PRACTICE TODAY (Jan. 14, 2016), http://www.lawpracticetoday.org/article/weary-of-wearables-ip-privacy-and-data-security-concerns/.

177. *See supra* Part I.B.

178. *See* Aran Khanna, *Stalking Your Friends with Facebook Messenger*, MEDIUM (May 26, 2015), https://medium.com/faith-and-future/stalking-your-friends-with-facebook-messenger-9da8820bd27d#.2xilbyymz (discussing a Harvard University student's discovery that Facebook Messenger allowed attaching a specific location to users of the application and subsequently created a map of exactly where a friend had traveled throughout the day).

would be shared, for example, with employers, governments, hackers, or thieves looking to target empty homes.

Despite the benefits accompanying wearable technology, a self-regulating industry promoting strict privacy practices would further benefit both the industry and its consumers. The self-regulating strategy should focus on the principles of clear and conspicuous notice, choice, and consent. Implementing these three principles sets a solid foundation for an emerging industry for three reasons. First, building notice, choice, and consent into the foundation of the regulation of wearable technology protects against regulatory agencies expanding their reach toward companies violating privacy concerns.[179] Second, structuring privacy principles to coincide with the existing European fundamental right to privacy opens American businesses up to compliant cyber interactions with European citizens and businesses.[180] Lastly, businesses can use a strict data privacy policy as a business advantage, as the instinctive privacy concern surrounding wearable technology comes to fruition as the industry grows.

A. The Solution: Notice, Choice, and Consent

In terms of privacy, as long as a business clearly informs consumers of what information is collected, what it is used for, and with whom it is shared, the business is in full compliance with current regulatory standards—for now.[181] The solution for respecting and protecting consumer privacy in this digital age revolves around three principles put in place in a self-regulating system: notice, choice, and consent. Although these principles seem basic, the FTC consent orders against major U.S. companies shed light on the rampant disregard for these principles, raising questions as to the effectiveness of protecting data privacy without legislation.[182]

The goal of providing notice is to fully educate an ordinary consumer. Consumers using wearable technology should receive notice of what information is collected and how that information will be used before the information is actually collected, which is most easi-

---

179. *See supra* Part I.G

180. *See supra* Part I.C–D.

181. *See* 16 C.F.R. §314.4 (2002); *SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach*, U.S. SEC. & EXCHANGE COMM'N (Sept. 22, 2015), http://www.sec.gov/news/pressrelease/2015-202.html (highlighting an Investment Advisor's failure to adhere to regulatory standards).

182. See *supra* Part I.G for a discussion of the consent orders against Google, Nomi Technologies, and Trendnet.

ly presented in the form of a privacy policy. Long gone are the days of companies having no privacy policy at all. Certain states, such as California, are on the forefront of U.S. data privacy by requiring any company that solicits business from a California resident to have a privacy policy in clear and conspicuous language.[183] Because the Internet is a global platform, all companies in the U.S. benefit from abiding by California data privacy laws, emphasizing the shift towards policies that aim to successfully inform ordinary consumers.

Wearable technology companies should implement clear, conspicuous, and accessible methods of informing consumers of its privacy practices. Such methods include having pop-up features, required scrollable content, and large, clearly readable text to force consumers to see privacy policies. These types of features put consumers on notice by informing them about the handling of their private information.

Choice is a key principle that, if implemented correctly, gives consumers real control over the fate of their personal data. Affirmative opt-in methods are most effective, as highlighted by the Safe-Harbor Framework.[184] For example, a wearable could ask users to affirmatively agree to have their geolocation tracked, rather than just including it in a privacy policy as an all-or-nothing approach. Users could also be given an affirmative option to chose with whom their information will be shared. Working legitimate choice options into the design of wearable technology will comply with existing regulatory agency standards, while increasing the chances of compliance with future standards.

Lastly, consent is paramount when dealing with private information. Wearable technology should implement easy methods of receiving initial consent, informing consumers of any changes, and regaining consent, and allowing consumers to withdraw their consent. The same features used for notice and choice apply to consent, like pop-up notifications and affirmative actions (such as clicking a box). Keeping consumers informed and maintaining accurate records of what consumers did and did not consent to are crucial to the privacy of wearable technology. Implementing these features encourages a high standard for privacy protection of information collected from wearables, and is ultimately attractive to both consumers and businesses.

183. *See* CAL. BUS. & PROF. CODE, §§ 22575–79 (West 2004).

184. *See supra* Part I.C. (discussing the EU Safe-Harbor).

B. Benefits of a Self-Regulating Industry on Improving Data Privacy in the U.S.

Raising the privacy standard through industry practices will help prevent the future consequences resulting from the astronomical amounts of data collected from wearable devices. The "unfair and deceptive business practices" standard is currently the heart of the regulatory enforcement against wearable devices and is likely to remain the focus of any enforcement in the future. Currently, companies found to have unfair and deceptive business practices clearly misled consumers or blatantly said one thing and did another in their privacy policies.[185] The future will require more than just truthful privacy policies.

With uncertainty under the law, companies will easily choose to provide only the bare minimum to avoid consent orders, but review of the current state, federal, and international legislation supports a much more aggressive approach to protecting privacy. The possibility of either a four percent fine on a company's gross annual income for failing to meet EU data privacy standards when collecting data from EU citizens[186] or exposure to liability for failing to comply with California data privacy requirements should be enough to spark data privacy protection.[187]

Respecting the public's value on personal privacy combined with offering more legitimate choices to consumers about what information their wearable devices are collecting is an invaluable strategy that pleases all types of consumers. The consumer who looks for more privacy in a device can opt-out of certain features and use the device according to his or her specific privacy terms, while the consumer who appreciates the advantages accompanying private data collection can choose certain features, including geolocation. In addition to attracting consumers, businesses can achieve regulatory compliance relatively inexpensively, especially considering the cost of complying with twenty-year consent orders,[188] paying a four percent fine on the gross annual income,[189] or paying damages from a lawsuit based on failure to comply with California state laws.[190]

---

185. *See, e.g.*, Google Consent Order, *supra* note 136.

186. Q&A Data Protection Reform, *supra* note 77.

187. See CAL. BUS. & PROF. CODE § 22575 (West 2004).

188. *See* discussion *supra* Part I.G.1–3 (providing an overview of the consent orders linked to Google, Nomi Technologies, and Trendnet).

189. Q&A Data Protection Reform, *supra* note 77.

190. *See* CAL. BUS. & PROF. CODE § 22575(a) (West 2004).

CONCLUSION

As the wearable device business grows to the predicted trillion-dollar industry, the amount of information collected from wearables grows at a similar rate. As more information is collected, the risks surrounding the security and privacy of that data increase. In the U.S., security receives the most attention, in terms of federal legislation, regulatory agencies, state-specific legislation, and industry standards. On the contrary, privacy of data lacks the attention it deserves. The majority of the data collected through wearable technology is unregulated under the sector-based approach to privacy, which only protects private information deemed worthy of separate legislation. Because the U.S. only holds businesses to a standard of not falling to unfair and deceitful business practices, regulating the privacy of data is mostly at the discretion of the business rather than controlled by the consumer.

Although the wearable technology market is growing during a time of virtually unregulated data collection in the U.S. (in comparison to the heavily regulated data collection under EU Law), the existing consent orders issued by regulatory agencies, the EU decision to issue fines for companies collecting information from EU citizens valuing up to four percent of that company's global income, and the growing public concern for personal data privacy demand that the U.S. self-regulating system to raise its privacy standards. Wearable technology companies should implement features that offer legitimate notice, choice, and consent, rather than wait for legislative or regulatory agency enforcement.

Preemptively raising privacy standards ahead of any regulation ultimately achieves better outcomes from both sides of the coin: Companies are able to protect themselves from heavy-handed regulatory agency enforcement, prepare for any possible new legislation, and cater to both EU and California law in this global market. Furthermore, all types of consumers benefit; consumers looking for more privacy are given the choice to consent to what information is collected and how it is used, while those consumers seeking the latest technological advances that use information collected from the body can choose that experience by affirmatively consenting. Today, it is essential for lawyers to counsel clients to incorporate data privacy into the design of wearable devices and to institute a default of increased data privacy in already existing products to successfully emerge in this rapidly growing technological industry.