Just What the Doctor Ordered: Protecting Privacy Without Impeding Development of Digital Pills

ABSTRACT

Using technology, humans are receiving more and more information about the world around them via the Internet of Things, and the next area of connection will be the inside of the human body. Several forms of "digital pills" that send information from places like the human digestive tract or bloodstream are being developed, with a few already in use. These pills could stand to provide information that could drastically improve the lives of many people, but they also have privacy and data security implications that could put consumers at great risk. This Note analyzes these risks and suggests that short-term improvements in warning and obtaining consent from consumers be implemented, while lawmakers carefully consider use constraints in order to both protect consumers and allow the development of what could be a highly beneficial form of technology.

TABLE OF CONTENTS

Experts estimate that in about ten years, up to one-third of Americans will be living with either a temporary or permanent device inside their bodies.[1] Humans have connected many of the objects they use in everyday life—from phones and cars to coffee makers and washing machines—to the Internet. This connectivity is known as the Internet of Things.[2] Connecting the human body to the Internet is the next logical frontier. Embedding technology into the human body makes sense given that mHealth, which refers to the use of mobile devices to support medical practice, is an area that is exploding in popularity.[3] These devices may come in many forms, but one form of internal device already taking shape is the digital pill. While the potential benefits are numerous, many skeptics cite serious risks to privacy that must be addressed.

There are already various pills in use and development that utilize technology to provide humans with information about what is going on inside of them. One example is the SmartPill, which measures pressure, pH levels, and temperature as it moves through patients' bodies to measure motility.[4] American doctors are also using the PillCam, a pill the size of a vitamin that contains small cameras and moves through the digestive tract in only a couple of hours, capturing images and transmitting them to an external data recorder, which allows patients to forego invasive, uncomfortable procedures.[5] By

1. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 104 (2014) (citing Cadie Thompson, *The Future of Medicine Means Part Human, Part Computer*, CNBC (Dec. 24, 2013, 8:00 AM), http://cnbc.com/id/101293979 [https://perma.cc/5XZK-5UF4]).

2. Jacob Morgan, *A Simple Explanation of the 'Internet of Things*,' FORBES (May 13, 2014), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#2dead45b6828.

3. 3 WORLD HEALTH ORG., *mHealth: New Horizons for Health Through Mobile Technologies*, *in* GLOBAL OBSERVATORY FOR EHEALTH SERIES, at 6 (2011), http://www.who.int/goe/publications/goe_mhealth_web.pdf [https://perma.cc/C7ZN-SLSQ].

4. Peppet, *supra* note 1, at 103 (citing *Motility Monitoring*, GIVEN IMAGING, http://givenimaging.com/en-us/Innovative-Solutions/Motility/SmartPill/Pages/default.aspx [https://perma.cc/G2RX-QS53]).

5. *PillCam Capsule Endoscopy*, GIVEN IMAGING, http://www.givenimaging.com/en-int/Innovative-Solutions/Capsule-Endoscopy/Pages/default.aspx [https://perma.cc/832Y-M3G8] (last visited Oct. 20, 2016); Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovatio*n, 21 RICH. J.L. & TECH. 6, 32 (2015).

making colon cancer screenings easier and more effective, this technology could also make them more prevalent.[6] Finally, a digital pill that prevents drunk driving is also being developed.[7] The pill would place a microchip into the bloodstream of the consumer that measures blood alcohol content when the person is in his car.[8] If the blood alcohol content is too high, the microchip will send a signal to the car, shutting it off.[9] If successfully implemented, this drug could prevent thousands of deaths that occur each year due to alcohol-impaired driving and could save up to $49 billion.[10]

Digital pills that combine ingestible microchip sensors with pharmaceuticals that are already in use have great potential for widespread adoption and high impact.[11] These drugs can operate in a number of ways. They can control and monitor the release of the active pharmaceutical ingredients after digestion.[12] They can record whether, when, where, and in what quantity the drug is released, as well as information about the physical state of the person taking the drug, such as temperature, activity level, heart rate, and respiration.[13] They also transmit signals and information about the patient to devices such as mobile phones, tablets and computers belonging to the patient, the patient's caregivers, or the patient's doctor.[14]

One company, Proteus Digital Health, is endeavoring to develop a digital pill that will measure and improve medication adherence and generally improve health outcomes for those prescribed long-term medications to treat chronic diseases.[15] An estimated 50% of patients

---

6. Thierer, *supra* note 5, at 32 (citing Joseph Walker, *New Ways to Screen for Colon Cancer*, WALL ST. J. (June 8, 2014, 4:54 PM), http://online.wsj.com/articles/new-ways-to-screen-for-colon-cancer-1402063124 [https://perma.cc/TZY5-Z8CV]).

7. Biz Carson, *Jawbone's CEO Sees a Future Where Tiny Sensors Travel in Your Blood*, BUS. INSIDER (Oct. 7, 2015, 7:48 PM), http://www.businessinsider.com/jawbone-ceo-hosain-rahman-imagines-bloodstream-wearables-2015-10 [https://perma.cc/66HM-XMKQ]; Jason Cipriani, *Jawbone Is Building a Health Tracker You Can Swallow*, FORTUNE (Oct. 8, 2015, 5:15 PM), http://fortune.com/2015/10/08/jawbone-ingestible-health-tracker/ [https://perma.cc/Z6QX-MDHV].

8. Carson, *supra* note 7.

9. *Id.*

10. *Impaired Driving: Get the Facts*, CTRS. FOR DISEASE CONTROL & PREVENTION (Nov. 24, 2015), http://www.cdc.gov/motorvehiclesafety/impaired_driving/impaired-drv_factsheet.html [https://perma.cc/T9AZ-N9KZ]; NHTSA, *Alcohol-Impaired Driving*, U.S. DEP'T OF TRANSP. (Dec. 2014), http://www-nrd.nhtsa.dot.gov/Pubs/812102.pdf [https://perma.cc/84WL-Z7LV].

11. Matthew Avery & Dan Liu, *Bringing Smart Pills to Market: FDA Regulation of Ingestible Drug/Device Combination Products*, 66 FOOD & DRUG L.J. 329, 330–32 (2011).

12. *Id.* at 331.

13. *Id.* at 331–32.

14. *Id.* at 332.

15. *US FDA Accepts Digital Medicine Drug Application for Otsuka and Proteus Digital Health*, BUS. WIRE (Sept. 10, 2015, 9:00 AM), http://www.businesswire.com/news

with chronic diseases in developed countries do not take their medication as prescribed.[16] This can cause relapse and recurrence of chronic diseases and results in an estimated $100–$300 billion in avoidable health care costs, both direct and indirect.[17] If successfully implemented, this new drug could significantly impact the way medication adherence is measured and, in doing so, could revolutionize the way that chronic disease treatment is tailored to individuals. The ability to measure medication adherence would allow health care professionals to more effectively tailor treatment of chronic diseases to individual patients, which could not only lead to better health outcomes, but also save billions of dollars in health care costs.[18]

Despite Proteus's potential for positive impact, there are significant drawbacks and possible barriers to its success. Privacy concerns already exist with regard to mHealth and the Internet of Things.[19] Therefore, these concerns will extend to the Proteus digital pill, which, as a digital ingestible sensor that sends daily information to a software application for mobile devices, qualifies as both. The concerns include a lack of certainty over which privacy laws and regulations apply to data created and transmitted using digital sensors, the insufficiency of the approaches to privacy preservation taken by current privacy laws, and the inherent security weaknesses of sensor devices. It is possible that, in response to these potential issues, the digital pill could fail before implementation as a result of precautionary overregulation of the use of information collected by the digital pill.

This Note addresses the privacy and data security issues that could stand in the way of the success of the Proteus digital pill and, in doing so, addresses how these issues could prevent implementation of ingestible sensors generally. Part I describes the development and potential benefits of the Proteus digital pill, as well as potentially applicable privacy and data security laws and regulations. Part II analyzes the application and adequacy of these laws and regulations in light of the actual privacy and security threats posed by the digital pill and the levels of privacy and data security desired by consumers. Part III offers a solution that would not only allow the digital pill to be implemented successfully to treat chronic diseases, but also provide

/home/20150910005497/en/U.S.-FDA-Accepts-Digital-Medicine-Drug-Application [https://perma.cc/B692-58Z9].

16. *Id*.

17. *Id*.

18. *Id*.

19. *See* Anne M. Helm & Daniel Georgatos, *Privacy and mHealth: How Mobile Health "Apps" Fit into a Privacy Framework Not Limited to HIPAA*, 64 SYRACUSE L. REV. 131, 158 (2014); Peppet, *supra* note 1, at 88–89, 129–33; *see also* WORLD HEALTH ORG., *supra* note 3, at 6.

consumers and health care providers with sufficient privacy and data security protection.

I. BACKGROUND

A. The Proteus Digital Pill

For several years, Proteus has been pioneering digital pill technology by developing its digital health feedback system, which consists of an ingestible sensor and external patch that collect and send information and a software platform that receives and displays that information. Proteus has been seeking regulatory approval of these projects and partnering with companies that are interested in using Proteus's ingestible sensor to improve health care delivery. The system is intended to improve treatment by creating an "integrated approach to patient-centric, anywhere, anytime mobile health products" in a number of areas of personal health, including cardiovascular disease; psychiatric, metabolic, and neurologic disorders; organ transplantation; and infectious disease.[20]

1. Development of the Ingestible Sensor

The Proteus sensor is one millimeter long and one-third of a millimeter thick—the size of a grain of sand.[21] It is made of silicon, copper, and magnesium that form a circuit with human stomach acid to power the microchip.[22] The microchip sends a signal to a patch worn on the abdomen skin that records and time-stamps the information.[23] The patch also collects other patient metrics, including whether the patient is resting, the angle of the patient's body, and the patient's patterns of activity.[24]

From the patch, information can be transmitted to the patient's smartphone or other Bluetooth-enabled device and then on to the

20. Press Release, Proteus Digital Health, Proteus Digital Health Announces FDA Clearance of Wireless Personal Health Monitor (Apr. 21, 2010), http://www.proteus.com/press-releases/proteus-announces-fda-clearance-of-wireless-personal-health-monitor/ [https://perma.cc/DL6E-QXYS] [hereinafter Press Release, Proteus Digital Health Apr. 21, 2010].

21. Russell Brandom, *The Frightening Promise of Self-Tracking Pills*, THE VERGE (Oct. 7, 2015, 11:16 AM), http://www.theverge.com/2015/10/7/9466121/proteus-digital-pill-tracking-privacy-quantified-self [https://perma.cc/XK8B-P988].

22. *Id*.

23. *Id*.

24. *See* Press Release, Proteus Digital Health, Proteus Digital Health Announces FDA Clearance of Ingestible Sensor (July 30, 2012), http://www.proteus.com/press-releases/proteus-digital-health-announces-fda-clearance-of-ingestible-sensor-2/ [https://perma.cc/2UM3-96UE] [hereinafter Press Release, Proteus Digital Health July 30, 2012].

patient's physician or caregiver, if the patient has consented.[25] The patient may view the information from the patch and sensor using a software application ("app") on her mobile phone or other device, and the physicians or caregivers may view the data via web portals.[26] Proteus has characterized these apps and web portals as "secure."[27]

In August 2010, Proteus Biomedical Inc. announced that it would affix the CE Mark to an ingestible sensor and monitor system, signaling Proteus's assertion that the system met European Union consumer and health requirements and could be marketed there.[28] In the United States, the Proteus Feedback System, which is solely an ingestible sensor independent of any other pharmaceutical drug, was approved by the United States Food and Drug Administration (FDA) for marketing as a medical device in July 2012.[29] In July 2015, the FDA expanded the Indications for Use statement for Proteus's ingestible sensors, allowing the device to be used to measure medication adherence and rendering it the only device with an FDA-approved claim for such measurement.[30] The FDA made this decision because the ingestible sensor records a quantifiable event: actual intake time.[31]

2. How the Ingestible Sensor Will Be Used

To be effective, the ingestible sensor and accompanying system must be combined with pharmaceutical products for which they can measure adherence. In January 2010, Proteus Biomedical and Novartis entered into an exclusive worldwide license and collaboration agreement to create pharmaceutical products that will utilize Proteus's sensor technology in the fields of organ transplantation, cardiovascular

---

25. *Id*.

26. *Id*.

27. *See* Ms. Smith, *FDA Accepts Application for Micro-Chipped Pill that Tells Doc if You Took Meds*, NETWORK WORLD: PRIVACY & SECURITY FANATIC (Sept. 14, 2015, 7:12 AM), http://www.networkworld.com/article/2983387/security/fda-accepts-application-for-micro-chipped-pill-that-tells-doc-if-you-took-meds.html [https://perma.cc/3UTK-QKRA].

28. Press Release, Proteus Digital Health, Proteus Biomedical Announces European CE Mark Approval of Ingestible Sensor and Monitor System (Aug. 13, 2010), http://www.proteus.com/press-releases/proteus-biomedical-announces-european-ce-mark-approval-of-ingestible-sensor-and-monitor-system/ [https://perma.cc/ET2J-EGED] [hereinafter Press Release, Proteus Digital Health Aug. 13, 2010].

29. Peppet, *supra* note 1, at 103–04*; see also* Press Release, Proteus Digital Health July 30, 2012, *supra* note 24.

30. Press Release, Proteus Digital Health, First Medical Device Cleared by FDA with Adherence Claim (July 2, 2015), http://www.proteus.com/press-releases/first-medical-device-cleared-by-fda-with-adherence-claim/ [https://perma.cc/F4QP-4G3N] [hereinafter Press Release, Proteus Digital Health July 2, 2015].

31. *Id*.

health, and oncology.[32] Proteus has also indicated to the European Medicines Agency (EMA) that it intends to use the digital pill to monitor medication adherence in patients with Type 2 diabetes, hypertension, Alzheimer's disease and hepatitis C, as well as patients who have been recently discharged from a hospital.[33] In April 2016, at the annual conference of the American College of Cardiology, Proteus shared that in a study of its digital feedback system, more than 84% of patients with uncontrolled hypertension and Type 2 diabetes using the combination of the digital sensor, the patch, and the app were able to reach their blood pressure targets, compared with only 33% of patients receiving usual care.[34] The first use of the digital feedback system outside of clinical settings in the United States will be by Barton Health, a health system in Lake Tahoe, California.[35] Barton will combine the sensor with generic medications for patients with uncontrolled and co-morbid hypertension.

Proteus is also seeking approval of a digital pill that will measure medication adherence in psychiatric patients. In July 2012, Proteus Digital Health and Otsuka Pharmaceutical Co. announced a license and collaboration agreement to develop medicines based on Otsuka's pharmaceutical products and Proteus's digital health feedback system in two therapeutic areas with high unmet medical needs.[36] Otsuka produces ABILFY, a drug used to treat schizophrenia, manic or mixed episodes occurring with bipolar I disorder, major

32. Press Release, Proteus Digital Health, Proteus Biomedical Announces License and Collaboration Agreement for Sensor-Based Pharmaceuticals (Jan. 12, 2010), http://www.proteus.com/press-releases/proteus-biomedical-announces-license-and-collaboration-agreement-for-sensor-based-pharmaceuticals/ [https://perma.cc/6YJ7-DNMS] [hereinafter Press Release, Proteus Digital Health Jan. 12, 2010].

33. *Draft Qualification Opinion*, EUROPEAN MEDICINES AGENCY 25 (Aug. 7, 2015), http://www.ema.europa.eu/docs/en_GB/document_library/Regulatory_and_procedural_guideline/2015/09/WC500193612.pdf [https://perma.cc/ZAA6-GTYL].

34. Stephanie Baum, *Proteus Digital Health Smart Pill Study Shows Significant Reduction in BP Levels*, MEDCITY NEWS (Apr. 4, 2016, 4:41 PM), http://medcitynews.com/2016/04/proteus-digital-health/?rf=1 [https://perma.cc/8TAZ-WAAD].

35. Jonah Comstock, *California Hospital Becomes First in US to Prescribe Ingestible Sensors from Proteus*, MOBIHEALTHNEWS (Jan. 11, 2016), http://mobihealthnews.com/content/california-hospital-becomes-first-us-prescribe-ingestible-sensors-proteus [https://perma.cc/9TSR-5M98].

36. Press Release, Proteus Digital Health, Proteus Digital Health, Inc. and Otsuka Pharmaceutical Co., Ltd. Announce Worldwide Agreement to Develop Novel Digital Health Products (July 5, 2012), http://www.proteus.com/press-releases/proteus-digital-health-inc-and-otsuka-pharmaceutical-co-ltd-announce-worldwide-agreement-to-develop-novel-digital-health-products-2/ [https://perma.cc/B4MV-RSC8] [hereinafter Press Release, Proteus Digital Health July 5, 2012].

depressive disorder, irritability associated with autistic disorder, and Tourette's Syndrome.[37]

On September 8, 2015, the FDA deemed the New Drug Application for a tablet containing ABILIFY embedded with a Proteus ingestible sensor to be sufficiently complete for substantive review.[38] Proteus and Otsuka are the first to submit an application for FDA-approved medication that contains an ingestible sensor.[39] In April 2016, the FDA issued a Complete Response Letter requesting additional information about the product's performance and any use-related risks that patients taking it might face.[40] Otsuka's executive vice president and chief strategy officer, Robert McQuade, stated that Otsuka and Proteus would work to provide the information the FDA has requested.[41]

B. Benefits of the Proteus Digital Pill

There are many benefits to be realized from the use of digital pills. Digital pills will alert doctors to whether a patient is taking his medication, when it is being taken, the patient's physical status at the time the medication is taken, and how the medication works in the patient's body.[42] The doctors and caregivers of a patient can thus both be alerted if that patient stops taking his medication and have access to general information about the patient's situation at the time he stopped taking the medication.[43] This is important for two reasons.

First, doctors administering medications to patients with chronic illnesses may be able to devise more effective treatment plans that are tailored to individual patients' needs after observing the medication adherence habits of the patients.[44] For example, patients are 3.5 times more likely not to take medications as prescribed if they

37. Otsuka Pharm. Co., *ABILIFY Medication Guide* (Aug. 2016), http://www.otsuka-us.com/products/Documents/Abilify.Medguide.pdf [https://perma.cc/UM3W-HET6].

38. Press Release, Proteus Digital Health, U.S. FDA Accepts First Digital Medicine New Drug Application for Otsuka and Proteus Digital Health (Sept. 10, 2015), http://www.proteus.com/press-releases/u-s-fda-accepts-first-digital-medicine-new-drug-application-for-otsuka-and-proteus-digital-health/ [https://perma.cc/P7NF-TKL3] [hereinafter Press Release, Proteus Digital Health Sept. 10, 2015].

39. *Id.*

40. Dominic Tyler, *FDA Knocks-Back Otsuka's Digital Pill Plans*, PMLIVE (May 6, 2016), http://www.pmlive.com/blogs/digital_intelligence/archive/2016/may/fda_knocks-back_otsukas_digital_pill_plans_1017143 [https://perma.cc/3Z69-GYPW].

41. *Id.*

42. *Id.*

43. *Id.*

44. Press Release, Proteus Digital Health July 5, 2012, *supra* note 36.

have reported having side effects from the medication.[45] If a doctor is alerted by the Proteus digital feedback system that the patient is not taking his medication, the doctor may be able to contact the patient, learn more quickly about the side effects the patient was experiencing, and adjust the patient's prescriptions so that he is more likely to take the medication.[46] Also, physicians may make costly and unnecessary changes in treatment when the physician is unaware that a patient who is not seeing results is actually just non-adherent.[47]

Second, medication non-adherence can negatively affect health outcomes.[48] For example, patients taking ABILIFY for schizophrenia or bipolar I disorder could be susceptible to manic and schizophrenic episodes if their medications are discontinued without the direction of a doctor.[49] The Proteus digital feedback system could be particularly helpful for these patients because they are often reluctant to let anyone know that they have stopped taking their medication.[50] For patients with high blood pressure, it has been shown that non-adherence can result in a 42% higher chance of chronic heart failure.[51] Diabetics who fail to adhere to their diabetes medications are 2.5 times more likely to be hospitalized than diabetics who regularly take their medications.[52]

If successfully implemented in treating patients with chronic diseases, the digital pill could have a significant economic impact on the health care industry by encouraging better adherence to prescription medications.[53] Medication non-adherence results in an estimated $100–$300 billion in avoidable direct and indirect health care costs, which represents 3% to 10% of total health care costs in the United States.[54] Nearly one in two Americans have chronic diseases, such as

---

45. *See Improving Prescription Medication Adherence Is Key to Better Health Care*, PHRMA (Nov. 18, 2014), http://www.phrma.org/publications/improving-prescription-medicine-adherence-is-key-to-better-health-care [https://perma.cc/ES2X-F5CC] [hereinafter PHRMA].

46. *Id.*

47. Comstock, *supra* note 35.

48. Aurel O. Iuga & Maura J. McGuire, *Adherence and Health Care Costs*, 7 RISK MGMT. & HEALTHCARE POL'Y 35 (2014), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3934668/ [https://perma.cc/Y8MT-DRAS].

49. Jonah Comstock, *Proteus, Otsuka Submit First Commercial Drug with Built-in Sensor to FDA*, MOBIHEALTHNEWS (July 2, 2015), http://mobihealthnews.com/46680/proteus-otsuka-submit-first-commercial-drug-with-built-in-sensor-to-fda [https://perma.cc/37DG-89E3].

50. Jonah Comstock, *FDA Expands Proteus Digital Health's Clearance to Include Measuring Medication Adherence*, MOBIHEALTHNEWS (July 2, 2015), http://mobihealthnews.com/44949/fda-expands-proteus-digital-healths-clearance-to-include-measuring-medication-adherence/ [https://perma.cc/JX9C-A8JM].

51. *See* PHRMA, *supra* note 45.

52. *Id.*

53. Press Release, Proteus Digital Health July 5, 2012, *supra* note 36.

54. Iuga & McGuire, *supra* note 48.

cardiovascular disease, asthma, depression, cancer, or diabetes.[55] Patients with these illnesses who do not adhere to their medications have higher health care costs than patients who do adhere to medications, resulting largely from hospital admissions, emergency room visits, and other inpatient costs.[56] Additionally, when these patients do not take their medications, insurance companies are wasting money on the unused drugs.[57]

Another benefit of the Proteus digital pill is that it can be used to accelerate, improve the accuracy of, and reduce the costs of clinical trials.[58] It is crucial to the success of a clinical trial that the participating patients adhere to the treatment being tested and evaluated.[59] Current methods for measuring adherence, including pill counts and patient questionnaires, are expensive, time-consuming, and imprecise.[60] Unsuccessful clinical trials can also result from an inability to determine inappropriate dosages; if the participating patient is not taking the medication, the researchers conducting the study will not know whether the dosage needs to be adjusted.[61]

Proteus intended the digital feedback platform to address both of these issues in clinical trials, in addition to its uses in treating patients.[62] In January 2015, Proteus integrated its digital feedback platform with Oracle Health Sciences Inform electronic data capture platform to create a cloud service that enables clinical trial sponsors to capture precise data about medication adherence in real time.[63] This move, as well as Proteus's request that the European Medicines Agency approve the use of its digital platform as a method for measuring adherence and physiological and behavioral parameters in clinical

55. *Id.*; *see also* PHRMA, *supra* note 45.

56. *See* PHRMA, *supra* note 45.

57. Robert Glatter, MD, *Proteus Digital Health and Otsuka Seek FDA Approval for World's First Digital Pill*, FORBES (Sept. 14, 2015, 8:09 AM), http://www.forbes.com/sites/robertglatter/2015/09/14/proteus-digital-health-and-otsuka-seek-fda-approval-for-worlds-first-digital-medicine/#25adffd94b5c.

58. *See* Comstock, *supra* note 49; Press Release, Proteus Digital Health, Oracle and Proteus Integrate Proteus Digital Health Feedback System with Oracle Health Sciences InForm to Help Increase Clinical Trial Accuracy (Jan. 12, 2015), http://www.proteus.com/press-releases/oracle-and-proteus-integrate-proteus-digital-health-feedback-system-with-oracle-health-sciences-inform-to-help-increase-clinical-trial-accuracy/ [https://perma.cc/3BND-WAMS] [hereinafter Press Release, Proteus Digital Health Jan. 12, 2015].

59. Press Release, Proteus Digital Health Jan. 12, 2015, *supra* note 58.

60. *Id.*

61. *Id.*

62. Press Release, Proteus Digital Health July 2, 2015, *supra* note 30.

63. Press Release, Proteus Digital Health Jan. 12, 2015, *supra* note 58.

trials, demonstrates that Proteus is actively seeking to use its technology to improve the efficiency and effectiveness of clinical trials.[64]

C. Current Laws Applicable to Ingestible Sensors

1. Privacy Laws

Privacy law in the United States began with limited common law torts designed to compensate victims actually injured by privacy invasion and has morphed into a broader statutory scheme that seems to recognize a right of privacy and is designed to prevent privacy harms.[65] Congress's approach to reducing the risk of privacy harm has been to categorize information according to its tendency to cause harm if disclosed and to regulate data that are considered riskier than other types of data.[66] The two types of data considered to be risky are personal information that lawmakers believe can be used to directly cause harm if disclosed and data that cannot be used to directly cause harm but can be used to reidentify anonymized data.[67] Because these types of data are regulated, lawmakers have relied on anonymization to protect consumer privacy.[68] The idea is that consumers will be protected against harmful uses of their personal information if organizations that collect data promise only to share those data in ways that are de-identified and anonymous.[69]

The federal statute that regulates privacy in health information is the Health Insurance Portability and Accountability Act (HIPAA).[70] The HIPAA Privacy Rule was published in 2000 and expanded in 2009 by the Health Information Technology for Economic and Clinical Health Act (HITECH).[71] Both the HIPAA Privacy Rule and HITECH mandated adoption of technology in health care and attempted to address the issues that such adoption would bring about for the privacy

---

64. Lisa Henderson, *Proteus Seeks EMA Approval on Ingestible Sensor*, APPLIED CLINICAL TRIALS (Oct. 16, 2015), http://www.appliedclinicaltrialsonline.com/proteus-seeks-ema-approval-ingestible-sensor.

65. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1732–34 (2010).

66. *See id*. at 1734.

67. *See id*. at 1735.

68. *See id*. at 1736.

69. *See* Peppet, *supra* note 1, at 129.

70. *See id*. at 139, 154; *see* Rachel V. Rose, *How Does HIPAA and the HITECH Act Impact Medical Device and Pharma Companies?*, BECKER'S HOSP. REV. (Jan. 11, 2013), http://www.beckershospitalreview.com/healthcare-information-technology/how-does-hipaa-and-the-hitech-act-impact-medical-device-and-pharma-companies.html [https://perma.cc/PZA2-Q2TF].

71. *See HIPAA Rules*, HIPAA SURVIVAL GUIDE, http://www.hipaasurvivalguide.com/hipaa-rules.php [https://perma.cc/HZ3V-LJG3] (last visited Oct. 26, 2016).

of patient health information.[72] The HIPAA Privacy Rule applies to covered entities, which are defined as health plans, health care clearinghouses, health care providers, and their business associates who transmit health information in electronic form in connection with a transaction covered by the Privacy Rule.[73] A business associate is a person or organization that is not part of a covered entity's workforce that performs certain functions on behalf of or provides certain services to covered entities when those functions or services involve the use or disclosure of protected health information.[74] Business associates include any persons that provide services for data transmission of protected health information to a covered entity and requires access on a routine basis to such protected health information.[75]

The Privacy Rule also only covers health information that qualifies as protected health information (PHI), defined as "individually identifiable health information that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium."[76] There are three elements that information must satisfy to be considered "individually identifiable health information."[77] First, the information must be either "created or received by a health care provider, health plan, employer, or health care clearinghouse."[78] Second, the information must relate to one of the following: "the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."[79] Finally, the information must either actually identify the individual or reasonably could be used to identify the individual.[80]

Health information that neither identifies nor provides a reasonable basis to identify an individual is de-identified health information (DHI).[81] There are two standards under which the U.S. Department of Health and Human Services (HHS) analyzes whether information could reasonably be used to identify an individual.[82] First,

72. *See id*.
73. 45 C.F.R. § 160.103 (2014).
74. *Id*.
75. *Id*.
76. *Id*.
77. *Id*.
78. *Id*.
79. *Id*.
80. *Id*.
81. OFFICE FOR CIVIL RIGHTS, *Summary of the HIPAA Privacy Rule* 4, HHS.GOV (May 2003), http://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/VA3A-XJBN] [hereinafter OCR, *Summary*].
82. Ohm, *supra* note 65, at 1737.

the statistical standard states that information is DHI if a statistician or someone with "appropriate knowledge . . . and experience" decides formally that the data are not individually identifiable.[83] Second, the safe harbor standard allows information to become DHI if the covered entity suppresses or generalizes eighteen enumerated identifiers, including generalizing birth dates to years and ZIP codes to the initial three digits of the code.[84] Information that qualifies as DHI can be used and traded without restriction of any kind.[85]

The HIPAA Privacy Rule sets forth requirements that limit the circumstances under which an individual's PHI may be used or disclosed by covered entities.[86] There are specific circumstances under which the Privacy Rule either permits or requires the disclosure or use of PHI, and PHI may be used or disclosed when the individual has authorized such use or disclosure in writing.[87] For example, PHI may be used or disclosed in the context of treatment, payment, research and public health activities.[88] Most state laws contrary to the HIPAA Privacy Rule are preempted.[89]

Section 13408 of the HITECH Act applies to organizations that both transmit PHI to covered entities or their business associates and require access to the PHI on a routine basis.[90] These organizations may include Health Information Exchange Organizations, Regional Health Information Organizations, E-prescribing Gateways, or vendors that contract with a covered entity to allow the covered entity to offer a personal health record (PHR) to patients as part of its electronic health record.[91] According to the American Health Industry Management Association, a personal health record is "an electronic, universally available, lifelong resource of health information needed by individuals to make health decisions."[92] PHRs can be populated by patients or by entities such as health care providers, insurers, and pharmacies.[93]

---

83. *Id*.

84. *Id*.

85. *Id*.

86. OCR, *Summary*, *supra* note 81, at 1.

87. *Id*. at 4.

88. *Id*. at 4–8.

89. *Id*. at 17.

90. Health Information Technology for Economic and Clinical Health Act § 13408, 42 U.S.C. § 17938 (2010).

91. *Id*.

92. Juliana Bell, *Privacy at Risk: Patients Use New Web Products to Store and Share Personal Health Records*, 38 U. BALT. L. REV. 485, 508 (2010); *see Role of the Personal Health Record in the EHR (2010 Update),* AHIMA (2010), http://library.ahima.org /xpedio/groups/public/documents/ahima/bok1_048517.hcsp?dDocName=bok1_048517 [https://perma.cc/9B3U-XMVP].

93. *See id.*

Under the HITECH Act, these organizations are considered business associates for purposes of HIPAA and must enter into Business Associate Agreements with the covered entities to which they transmit PHI.[94]

Consumer protection laws like the Federal Trade Commission Act (FTC Act) provide another method for protecting privacy.[95] This act is not specific to health information, but has been applied to mobile apps.[96] The FTC Act gives the Federal Trade Commission (FTC) the power to regulate marketing practices and deceptive advertisements.[97] This has allowed the FTC to pursue cases against app developers who engage in practices that are contrary to the privacy policies published about the apps.[98] For example, the Path social networking app automatically collected and stored information that was gathered from app users' mobile devices, even if a user had declined to give the app permission to do so.[99] The FTC sued Path's operators for this violation of the FTC Act, as well as for making misrepresentations in its privacy policy and collecting personal information from children without parental consent; under its settlement with the FTC, Path had to pay an $800,000 fine and institute a comprehensive privacy program that included periodic privacy assessments.[100]

Another type of privacy law that has been suggested but not yet widely implemented with respect to the Internet of Things is "use constraints."[101] Rather than relying on anonymization, use constraints directly limit different parties' abilities to collect, store, and use specific types of data.[102] An example of a use constraint that already exists is some state legislatures' having passed laws limiting employers' consideration of applicants' credit reports.[103]

In the context of information privacy, use constraints could take several forms.[104] They could limit cross-context use of information data

94. Rose, *supra* note 70.

95. *See* Helm & Georgatos, *supra* note 19, at 158–59.

96. *Id*.

97. *Id*. at 159.

98. *Id*. at 160.

99. *Id*.

100. *Id*. (citing Press Release, Fed. Trade Comm'n, Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), https://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived [https://perma.cc/5UNS-HL9Y]).

101. *See* Peppet, *supra* note 1, at 150–57.

102. *See* Melissa W. Bailey, *Seduction by Technology: Why Consumers Opt out of Privacy by Buying into the Internet of Things*, 94 TEX. L. REV. 1023, 1052 (2016).

103. *See* Peppet, *supra* note 1, at 151–52.

104. *See id*. at 150–57.

whereby, for example, employers, insurers, or other economic actors can use data about an individual to draw inferences that allow them to discriminate against these individuals on the basis of race, gender, age, or economic status.[105] Use constraints could also prevent forced disclosure of specific information.[106] For example, a handful of states have passed laws that restrict insurance companies from requiring that an insured disclose the data collected by the Event Data Recorder in the insured's automobile.[107] Some states have advocated for the implementation of use constraints in the arena of Internet of Things data, but currently few have enacted such laws and those that exist are narrowly tailored.[108]

2. Data Security Laws

In the United States, there is no general federal data security statute, and data security is regulated via the FTC Act and state data breach notification laws.[109] Data security with regard to health information is also regulated by the HIPAA Security Rule.[110] The FTC Act gives the FTC the power to prevent people and entities from using "unfair or deceptive acts or practices in or affecting commerce."[111] This mandate has given rise to two types of enforcement cases: deception and unfairness.[112] Deception cases arise when a company violates security-related statements it has previously made to consumers.[113] For example, the FTC brought an action against web-enabled camera manufacturer TRENDnet after a Houston couple's baby monitor was hacked.[114] Even though TRENDnet had promised customers that its cameras were secure, the male hacker was able to shout expletives at the baby through the camera.[115] This was the FTC's first action against an Internet of Things manufacturer, and it resulted in a consent order with TRENDnet requiring the implementation of a rigorous security program to address risks and protect consumers' information.[116]

---

105. *Id*. at 151.
106. *Id*. at 153.
107. *See id*. at 154–55.
108. *See id*. at 150–57.
109. *See id*. at 136–37.
110. *See* Helm & Georgatos, *supra* note 19, at 154–55.
111. 15 U.S.C. § 45(a)(2) (2012).
112. *See* Peppet, *supra* note 1, at 136–37.
113. *See id*.
114. *Id*. at 135.
115. *Id*.
116. *See* TRENDnet, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 78 Fed. Reg. 55,717 (Sept. 11, 2013) (describing the complaint against, and consent order with,

The other type of data security cases the FTC has brought are unfairness cases.[117] In order to declare an act or practice unfair, the FTC must show that the act or practice 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."[118] The FTC may also use public policy to support the contention that a practice is unfair.[119] In the health care industry, HIPAA could serve as a sufficient public policy, making it easier for the FTC to establish a case of unfair practice with regard to data security.[120] Even in contexts where there are no federal statutory requirements about data security, the FTC has been able to successfully argue that it has jurisdiction to bring an enforcement action over unfair data security practices, suggesting that this jurisdiction is rather broad.[121]

In addition to FTC regulation, forty-six states have data breach notification statutes.[122] These statutes require notification when security breaches result in the theft of records containing "personal information"—a combination of an individual's first and last name and either the individual's Social Security Number, driver's license number, or bank or credit card account information.[123] While the majority of states do not mention health information in their data security statutes, eight states have specifically included it in their definitions of personal information.[124] Arkansas, California, Missouri, and Puerto Rico include "medical information."[125] Iowa, Nebraska, Texas, and Wisconsin include a person's "unique biometric data."[126]

Finally, in the health care industry, the HIPAA Security Rule and the American Recovery and Reinvestment Act of 2009 ("Recovery Act") regulate data security.[127] The Security Rule applies to the same

---

TRENDnet); Press Release, Fed. Trade Comm'n, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (proposed Sept. 11, 2013), http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles [https://perma.cc/5862-99HC].

117. *See* Peppet, *supra* note 1, at 137.

118. 15 U.S.C. § 45(n) (2012).

119. *Id*.

120. *See* Peppet, *supra* note 1, at 137.

121. *See id*.; *see also* FTC v. Wyndham Worldwide Co., 799 F.3d 236, 243–49 (3d Cir. 2015) (holding that the FTC has authority to bring an enforcement action over hospitality company's data security-related practices).

122. *See* Peppet, *supra* note 1, at 137.

123. *Id*. at 137–38.

124. *Id*. at 138–39.

125. *Id*. at 138.

126. *Id*. at 139.

127. *See* Helm & Georgatos, *supra* note 19, at 154; *see also* Daniel J. Gilman & James C. Cooper, *There Is a Time to Keep Silent and a Time to Speak, the Hard Part Is Knowing Which Is*

entities and information as the HIPAA Privacy Rule, and it was designed to be flexible and technologically neutral enough to apply to new technology.[128] The rule requires that covered entities implement administrative, physical, and technical safeguards that will achieve four objectives: guarantee the confidentiality of PHI that a covered entity creates, receives, or transmits; identify and protect against reasonably anticipated security threats to PHI; protect against reasonably anticipated impermissible uses or disclosures; and guarantee compliance by the entity's workforce.[129]

Further, HITECH requires entities covered by HIPAA to notify both the affected individuals and HHS upon discovering that there has been a breach of unsecured PHI.[130] HHS must post a list of covered entities that have reported such breaches of PHI involving more than 500 individuals, and if over 500 residents of a state or jurisdiction have been affected, the covered entity must alert the media in that state or jurisdiction.[131] For vendors of personal health records, who may not be covered by HIPAA, the Recovery Act requires that, following the discovery of a security breach of PHR identifiable health information, the vendor must notify each individual whose information was accessed and the FTC.[132]

II. ANALYSIS

A. Lack of Clarity over Applicable Privacy Laws

It is not clear which privacy laws will actually apply to digital pills. The HIPAA Privacy Rule applies only to individually identifiable health information that is stored or transmitted by "covered entities" and their "business associates."[133] Covered entities are usually health care providers, health insurers, or health care clearinghouses that process billing information, not pharmaceutical companies.[134] Pharmaceutical companies can be considered "business associates" if they perform "functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of protected health

Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information, 16 MICH. TELECOMM. & TECH. L. REV. 279, 304 (2010).

128. *See* Helm & Georgatos, *supra* note 19, at 154–55.

129. *Id*.

130. *See id*. at 155.

131. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (proposed Aug. 24, 2009); Helm & Georgatos, *supra* note 19, at 153–56.

132. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13407, 123 Stat. 115, 269–70.

133. *See* Bell, *supra* note 92, at 488, 511.

134. 45 C.F.R. § 160.103 (2014).

information."[135] It is possible that Proteus could be seen as performing functions, activities, or services for health care providers who receive the information transmitted from the digital pill. If so, Proteus would be required to enter into business associate contracts with each covered entity for which it performs functions or activities—a cumbersome practice that it seems unlikely a company would put itself in a position to have to do.[136]

On the other hand, Proteus may not actually be providing a service to covered entities. Proteus allows patients to access information transmitted by a pill.[137] Doctors only receive the information if the patient allows the doctor to access a web portal.[138] It is possible that Proteus would not be considered a business associate subject to the HIPAA Rules because it is only providing a service to the patient, not to a covered entity.[139] In fact, because patients can choose to keep the information to themselves, the information sent from a patient's digital pill could potentially never reach a covered entity at all.

As Proteus is a vendor of PHRs that may be accessed by covered entities, it is possible that Proteus could be covered by Section 13408 of the HITECH Act.[140] It is more likely, though, that Proteus's provision of PHRs will escape such regulation because Proteus will not be contracting with health care providers to allow them to offer personal health records to their patients.[141] Instead, Proteus will provide PHRs to individual patients who may or may not choose to then share their personal health records with their physicians, possibly not implicating a covered entity at all.[142] Where an entity operates systems that provide PHRs directly to consumers rather than handling the information under the provisions of a business associate agreement with a covered entity, many experts agree that there is a gap in HIPAA coverage.[143] The Proteus digital pill could fall into that gap and, consequently, the information collected by Proteus will not be subject to HIPAA's rules regarding handling, storing, and transmitting of

135. *See* Rose, *supra* note 70.

136. *See* OFFICE FOR CIVIL RIGHTS, *Covered Entities and Business Associates*, HHS.GOV (last visited Sept. 5, 2016), http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/CHA8-XLGK] [hereinafter OCR, *Covered Entities*].

137. *See* Ms. Smith, *supra* note 27.

138. *See id*.

139. *See* Rose, *supra* note 70.

140. 42 U.S.C. § 17938 (2012).

141. *See* Rose, *supra* note 70.

142. *See* Ms. Smith, *supra* note 27.

143. *See* Bell, *supra* note 92, at 511; *see also* Gilman & Cooper, *supra* note 127, at 304 n.125.

information. Instead, those seeking protection or redress for privacy and data security-related issues will have to look to the myriad varying state regulations concerning these topics, the "deception" and "unfairness" prongs of the FTC Act, and the data breach requirements for PHR vendors under the Recovery Act.

B. Shortcomings of Anonymization

Even if HIPAA or a more stringent state privacy statute or regulation does apply to Proteus, the personal information of digital pill consumers could be at risk. According to Paul Ohm, "almost every single privacy statute and regulation ever written in the U.S. and the EU embraces—implicitly or explicitly, pervasively or only incidentally—the assumption that anonymization protects privacy."[144] Privacy and data security statutes and regulations frequently offer safe harbors to entities that anonymize their data.[145] For example, under HIPAA, there are no restrictions on the use and disclosure of DHI.[146] Now, due to advances in computer science, it is possible to reidentify databases that were supposedly protected using anonymization, and this fact weakens the protections that these laws and regulations provide to consumers and their information.[147] One study found that 87% of Americans could be uniquely identified using the combination of their ZIP code, birth date, and sex.[148]

In 2006, it was discovered that users could be easily identified in an anonymized database released by Netflix.[149] Netflix had released one hundred million records to reveal how its users had rated movies from December 1999 to December 2005.[150] Although Netflix had removed identifying information, those with access to the database could see the movies each user rated, the dates they rated them, and the rating they assigned.[151] Researchers from the University of Texas found that it would be extremely easy for someone who has only a little information about a person in the database to reidentify that person.[152] Anyone seeking to reidentify another person in a dataset would need to know outside information about that person, such as the movies that person rated, but such outside information may not be so difficult to

144. Ohm, *supra* note 65, at 1740.
145. *Id*.
146. OCR, *Summary*, *supra* note 81.
147. *See* Ohm, *supra* note 65, at 1740; *see also* Peppet, *supra* note 1, at 129.
148. *See* Ohm, *supra* note 65, at 1705.
149. *Id*. at 1720–21.
150. *Id*. at 1720.
151. *Id*.
152. *Id*. at 1721.

find.[153] Ohm warns that in a world "awash in data about people," it is "naïve to assume that the adversary will be unable to find the particular piece of data needed to unlock anonymized data."[154] Further, health information, even if subject to the anonymization standards under HIPAA, may be especially vulnerable; the eighteen identifiers that must be suppressed for data to be DHI under the safe harbor standard do not include other identifiers that could be used to reidentify a dataset, including hospital name, diagnosis, year of visit, patient's age, and the first three digits of the ZIP code.[155] These bits of information could be used to reidentify datasets that have been supposedly anonymized and qualify as DHI under HIPAA.[156]

The information transmitted by a Proteus digital pill may be even more susceptible to re-identification. Sensors capture a wide variety of data that can paint a detailed portrait of an individual, rendering each individual in a sensor-based dataset unique.[157] This makes sensor datasets highly sparse, meaning that individuals in the dataset can be separated from the other individuals using only a few attributes.[158] Sparse datasets are extremely difficult to anonymize.[159] To demonstrate this difficulty, MIT researchers discovered that by locating individual users in a dataset within several hundred yards of a cell-phone transmitter over the course of an hour on four occasions in one year, they could identify 95% of the users in the dataset.[160] The dataset contained anonymized data created by location-oriented sensors on 1.5 million cell phone users in Europe over fifteen months.[161]

These demonstrations of the ease of re-identification of anonymized datasets should impress upon regulators and lawmakers that laws and regulations that seek to protect privacy by requiring anonymization, such as HIPAA's Privacy Rule, are inadequate, especially as they concern sensor technologies like Proteus's digital pill. Some regulators, such as the FTC, have sought to redefine information along a spectrum of identifiability, rather than simply grouping information into two categories: personally identifiable and not

153. *Id*. at 1721, 1724.

154. *Id*. at 1724.

155. *Id*. at 1740

156. *Id*.

157. Peppet, *supra* note 1, at 130.

158. *Id*.

159. *Id*.

160. *Id*. at 131 (citing Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCI. REP. (Mar. 25, 2013), http://www.nature.com/articles/srep01376 [https://perma.cc/98XR-WC8N]).

161. *Id*.

personally identifiable information.[162] Along a spectrum of this sort, non-identifiable information would not be regulated.[163] Information that clearly identifies individuals would be heavily regulated, similar to PHI under the HIPAA Privacy Rule, and potentially identifiable information would be subject to less stringent limits on use and disclosure.[164] The FTC listed three standards that, if met, would render data outside the scope of the FTC's regulation: the dataset is not reasonably identifiable, the company that owns the dataset commits not to reidentify the data, and the company requires downstream users of the data to commit not to reidentify the data.[165]

Some still find this approach inadequate; they argue that determining whether data are reasonably identifiable will be impossible.[166] As Ohm puts it, "No matter how effectively regulators follow the latest re-identification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered."[167] This may be particularly true for sparse datasets generated by sensors like the Proteus digital pill.[168] It is impossible to know the kinds of information that new technologies may be able to pull from human bodies in the coming years. Due to the threat of re-identification, all of the information in these datasets may need to be termed personally identifiable information, but current laws and regulations will only protect certain types of information.[169]

C. The Incompatibility of Notice & Consent and the Digital Pill

In addition to relying on anonymization, policymakers have embraced notice and choice as their principal method for regulating the Internet.[170] Notice and choice is essentially consumer consent in the context of the Internet in which a firm provides information to the consumer, usually in the form of a privacy policy, and then allows the consumer to either accept or reject its services.[171] With devices like the

---

162. Peppet, *supra* note 1, at 132–33 (citing FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 22 (2012)).

163. *See id.* at 132.

164. *Id.*

165. *Id.* at 132–33 (citing FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 22 (2012)).

166. *See generally* Ohm, *supra* note 65, at 1742.

167. *Id.*

168. *See* Peppet, *supra* note 1, at 133.

169. *Id.*

170. *Id.* at 140.

171. *Id.* at 141.

digital pill, this approach to informing consumers about and gaining their agreement to a company's information gathering processes is highly problematic. First, logistically, there is no way to display a privacy notice on a digital pill containing a sensor.[172] Companies providing devices, including wearables like the Fitbit, have had to find other methods of presenting a privacy policy to their consumers for acceptance, such as including a policy in the box the device comes in, having the policy on the company website, and conveying the policy via a mobile application associated with the device.[173]

Even when companies can pull together a privacy policy and offer it to consumers in a medium separate from the data-collecting device, privacy policies are essentially complicated legal documents, and therefore often cannot accurately and understandably describe what information the device is collecting and how the company is using that information.[174] When companies offer privacy policies via mobile applications, they often apply only to the use of the app and therefore run the risk of failing to provide adequate information about the separate sensor device.[175] Further, it seems that technology may have outgrown the concept of a privacy policy as the vast amount of data that devices such as the digital pill are able to collect renders drafting a sufficiently descriptive privacy policy almost impossible.[176] There are many possible misuses that consumers will not be able to read about in a privacy policy.[177] Even the Obama administration has acknowledged that there will be instances in which the notice and consent framework will no longer function adequately to protect consumers and allow them to make meaningful choices about their personal information and how it is shared.[178] The inadequacy of notice and consent is perhaps more concerning than the lack of privacy regulation because it impedes consumers' abilities to make educated decisions about what devices they will use and how they will share their information. Even if a device is unsecure or discloses consumers' personal information, the consumer may decide that the benefits of the device outweigh these drawbacks, but if consumers have no way of knowing what the risks are, the consumers' autonomy to make meaningful choices disappears.

---

172. *Id.*; Thierer, *supra* note 5, at 32.

173. Peppet, *supra* note 1, at 141.

174. *See id.* at 142.

175. Peppet, *supra* note 1, at 142.

176. Thierer, *supra* note 5, at 62–63.

177. *Id.* at 80.

178. *Id.* at 71 (citing EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/H47A-NJ9M]).

D. Difficulty of Securing Sensor Data

Computer-security experts agree that smaller, sensor-based devices are easier to hack than devices with a less compact form.[179] Among examples of devices that would be prone to data security problems are the Fitbit fitness tracker, digital insulin pumps, and baby monitors equipped with internet connection and cameras. A research team from Florida International University showed that the Fitbit data could be captured using simple tools from within fifteen feet.[180] Another security researcher proved that insulin pumps that communicated wirelessly to a monitor used by diabetics to check insulin levels could be easily accessed by hackers seeking to cause the monitor to display inaccurate information that would lead the diabetic to administer the wrong dose.[181]

In addition, devices that are compact are said to have a "small form factor," and while this may render devices more convenient to consumers, it often also renders the device much harder to secure.[182] It is difficult to include the processing power or the battery life needed to support robust security measures like encryption devices with small form factors.[183] Finally, devices like computers and smartphones boast operating systems that can be updated remotely by software companies to fix security problems after they have been released into the market to protect against new threats and keep up with new security developments.[184] Small sensor devices do not usually have such operating systems and therefore cannot be updated to secure the device.[185]

E. Potential Consequences of Privacy and Data Security Issues Facing the Digital Pill

Even though the Proteus digital pill's data may be difficult to secure, potentially weak data security may not be as great a problem as it sounds. First, Proteus will have its own private incentives for bolstering data security.[186] Both public and privately-held companies likely suffer great financial losses when breaches occur, and firms generally suffer more financially from identity fraud than do

179. Peppet, *supra* note 1, at 135.
180. *Id*. at 134.
181. *Id*.
182. *Id*. at 135.
183. *Id*.
184. *Id*.
185. *Id*.
186. Gilman & Cooper, *supra* note 127, at 331.

consumers.[187] Second, there is evidence that the risk of harm to consumers from data breaches is low.[188] A survey of consumers who had received breach notifications found that only two percent of those consumers had suffered any kind of identity fraud.[189] Medical identity theft is even more rare.[190]

Also, existing laws and regulations could address data security issues. Where data security measures are deceptive or unfair, the FTC Act applies and the FTC has been active in enforcing cases under both prongs.[191] Many states have data breach notification laws, as well, and even if Proteus were not required to adhere to rules about data security measures and breach notification under HIPAA, the Recovery Act would require Proteus, as a PHR vendor, to notify consumers and the FTC in the event of a breach.[192]

The privacy issues regarding the digital pill pose a greater threat than the data security issues. First, it is unclear which privacy laws will apply to the Proteus digital pill. If HIPAA does not apply to the Proteus digital pill, Proteus could use and disclose its consumers' information in a variety of ways that consumers would deem harmful. Second, even if laws such as the HIPAA Privacy Rule do apply to the Proteus digital pill, consumers' information and identities could still be compromised due to re-identification. In either scenario, consumers' personal information may fall into hands that the consumers would not want their information falling into and that may use the information in ways that would be harmful to consumers.

Medical information is unique in that it is both highly personal to patients and valuable to businesses.[193] For example, medical information companies use pharmacy data to track drug prescriptions and provide pharmaceutical companies and financial analysts with information about pharmaceutical demand.[194] Employers also have an interest in gleaning medical data about their current and potential employees that they can use to make personnel decisions, and they could easily turn to a company like Proteus for those data.[195] Data from sensors such as the Proteus digital pill could also be used by insurers to

187. *Id*. at 331–32.

188. *Id*. at 324.

189. *Id*.

190. *Id*. at 320.

191. *See* Peppet, *supra* note 1, at 135–37.

192. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13407; Helm & Georgatos, *supra* note 19, at 154–55.

193. *See* Bell, *supra* note 92, at 488.

194. *Id*. at 488–89.

195. *See* Peppet, *supra* note 1, at 118–20.

set insurance premiums, lenders to assess creditworthiness, and retailers to price discriminate.[196] The Proteus digital pill tracks general health statistics about the patient taking the pill as well as whether that patient, who presumably has a chronic disease, is taking her medication as prescribed.[197] This could be valuable to parties making decisions about that patient.[198] As Juliana Bell points out, "[t]he disclosure of medical information, whether inadvertent or not, can lead to embarrassment, ostracism, job loss, difficulty obtaining health insurance, and health care fraud."[199] Equally important is the harm that lack of privacy may cause to a consumer's notions of personal liberty and autonomy.[200]

These privacy and data security issues could lead to the inability of drug companies to provide products such as the ingestible sensor due to legal uncertainty or precautionary overregulation.[201] Policymakers, anticipating harms that could result from the gaps in privacy law, the inadequacy of data anonymization, and the potential weakness of data security measures, may be moved to enact laws and regulations that preemptively ban certain uses of data from the Proteus digital pill or require Proteus to seek certain permissions.[202] Such measures could prevent more benefit than harm.[203] The Proteus digital pill and other ingestible sensors have the potential to significantly improve the welfare of individuals and society by improving health outcomes for chronically ill patients and reducing health care costs.[204] These improvements may never be realized, though, if unnecessarily strict regulations are imposed on these new technologies.[205] Such regulations tend to reduce the ability of companies to produce new products, maximize the quality of these projects, and provide these products at a reasonable price.[206] Rather than predicting all possible worst-case scenarios and imposing precautionary restraints to prevent these scenarios from occurring, policymakers should utilize such

196. *See id*. at 123.

197. See Brandom, *supra* note 21; Press Release, Proteus Digital Health July 5, 2012, *supra* note 36.

198. *See* Peppet, *supra* note 1, at 118–20.

199. Bell, *supra* note 92, at 489.

200. Gilman & Cooper, *supra* note 127, at 316.

201. *See*, *e.g.*, *id*. at 332–34; Thierer, *supra* note 5, at 46–49.

202. *See* Thierer, *supra* note 5, at 49.

203. *See id*. at 47.

204. Press Release, Proteus Digital Health July 30, 2012, *supra* note 24.

205. *See* Thierer, *supra* note 5, at 53.

206. *See id*. at 55.

precautionary regulations only when an immediate and extreme threat to privacy and security has been clearly established.[207]

III. SOLUTION

It is clear that a balance must be struck to mitigate between the risk of overregulation that could destroy the benefits offered by digital pills and the privacy risks that this technology presents to consumers. Some have suggested that where the privacy and security risks posed by a technology are great and the ability of consumers to adequately gain notice and give consent to the information practices of a company are diminished by incompatibility with the traditional privacy policy paradigm, the regulatory response should be to impose "use constraints."[208] Rushing to enact legislation or regulations that limit how third parties can use private data should not be the answer, though. Such regulation would bypass consent and impose restrictions on the ways that companies and the third parties with whom they share data can utilize information.[209] Although constraints on some uses may eventually provide a solution to the privacy and data security issues posed by ingestible sensors, use constraints should only be imposed after a thorough cost-benefit analysis has been undertaken to examine the potential benefits of the information extracted from the digital pill against the risks of use of this information, and such analysis could take years.

Although there is a lack of clarity as to what privacy laws will apply to digital pills, there is evidence that risks, such as identity fraud, are low.[210] If the risks are low and the consequences are mild, the cost of overregulation may be too high to justify use constraints. People in today's society readily accept the loss of their privacy in exchange for efficiency, convenience, and small price discounts. The digital pill has the potential to provide vast benefits to doctors and patients alike and to alleviate the astronomical cost of health care. Caution must be taken before regulating such technology out of existence.

Until an accurate analysis of the costs and benefits associated with the information that can be gleaned from ingestible sensors by companies like Proteus is conducted, it is clear that some precaution must be taken to afford consumers an adequate level of protection.

---

207. *Id*.

208. *See generally* Peppet, *supra* note 1, at 150; Thierer, *supra* note 5, at 71 (citing EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/H47A-NJ9M]).

209. *See* Peppet, *supra* note 1, at 150.

210. *See* Gilman & Cooper, *supra* note 127, at 320, 324.

Because of the uncertainty as to what laws apply to the digital pill, the most pertinent risk to consumers using such technology is that they will not be able to understand or control what information Proteus is collecting and how that information is being used. With this in mind, the precautions that should be put in place must improve upon the notice and consent model. One potential improvement would be to adapt a more rigorous method of affording patients a meaningful choice by utilizing informed consent.

Before any physician treats a patient, that physician must obtain informed consent.[211] According to the doctrine of informed consent, when physicians make a treatment recommendation, they must disclose to patients the risks and benefits of the proposed treatment, as well as any realistic, available, alternative treatments or no treatment at all, before it can be said that the patient has given his or her informed consent to treatment.[212] Doctors prescribing the digital pill could be required to inform patients about the privacy and data security risks inherent in the pill. They would describe what information is being collected and list the types of third parties to whom that information is being sent. The consumer would then be allowed to consider this information, and if she chooses to fill the prescription for the pill, then she would be manifesting her consent.

Using the framework of informed consent in the context of digital pills has many advantages. First, unlike providing a privacy policy for the consumer to read when the consumer opens the mobile application associated with the pill, informed consent allows the consumer to consider privacy concerns when she is still talking to her doctor, she has not yet made the decision as to whether to take the digital pill, and importantly, she has not yet paid for the pill. This affords the consumer greater control and more opportunity to decline. Second, when a consumer swipes through a privacy policy on an app for a product that she has already purchased, she is probably less likely to pay attention to the terms than if she is speaking to someone trusted, like a doctor, who is explaining those terms.

There are some reasons this approach may not work. First, it may be difficult for a doctor to verbally convey information that is difficult to convey even using a written document. Doctors may also balk at the suggestion that they take the time to explain the privacy costs and benefits to patients. There may even be suggestions that if

211. Marc D. Ginsberg, *Informed Consent and the Differential Diagnosis: How the Law Can Overestimate Patient Autonomy and Compromise Health Care*, 60 WAYNE L. REV. 349, 352 (2014).

212. *Id*. at 353.

physicians convey this information, they could be sued by patients whose privacy is later compromised.

On the other hand, doctors will be willing to take the extra time to offer this information to their patients because of the immense benefits they stand to gain from understanding the medication adherence habits of their patients. There are ways to simplify the information that needs to be conveyed to patients deciding whether to use a digital pill. What physicians tell their patients could be crafted by Proteus and other future digital pill manufacturers so that physicians are essentially rehearsing a script. This would make the digital pill very similar to any other prescription medication that requires physicians to lay out the risks and side effects before prescribing to patients. The information could also be conveyed in a video that patients watch in the doctor's office so that doctors do not have to give up precious time.

Further, it is unlikely that doctors would be found liable in a malpractice case for any privacy or data security-related harm that a patient experienced from using a digital pill simply because they informed the patient of these risks; doctors in this situation would likely not be providing care that falls below the standard of care. Doctors can also be protected by having patients sign waivers that release them from liability regarding the privacy and data security risks of the digital pill.

Finally, using an informed consent model will avoid damage to consumers' notions of autonomy and liberty by giving them greater choice, and it will sidestep the risk of privacy laws becoming too paternalistic.[213] In the end, regulations that constrain specific uses may be necessary, but by strengthening methods for obtaining consent and granting consumers a meaningful choice while deciding whether use constraints should be used and what uses should be constrained, legislators and regulators can avoid being viewed as overprotective and allow a potentially beneficial technology to develop.

IV. CONCLUSION

Ingestible sensors have great potential to provide benefits both financial and health related. The risks of the digital pill with regard to privacy and data security may lead some to cry for preemptive regulation. Those who argue for regulation and legislation, such as use constraints, should exercise caution, though, and truly examine the implications of regulation and the desires of consumers. Rather than immediately limiting information use, policymakers should focus on

213. *See* Thierer, *supra* note 5, at 68.

improving the methods by which consumers can be educated and give consent. If they do so, they will encourage the development of technology with great potential, and they will promote the values of liberty and autonomy that Americans hold dear.

Amelia R. Montgomery[*]

[*] J.D. Candidate, Vanderbilt Law School, 2017; B.A., Davidson College, 2012. The author would like to thank her parents, Robert and Regina Montgomery for their love, support and the examples they have set for her throughout her life and especially throughout her education. The author would also like to thank the staff of the VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW, particularly Sarah Dotzel and Nicole Kalkines for their effort and suggestions.