Nova Law Review

Volume 39, *Issue* 3 2017 *Article* 6

Care And Feeding Of Privacy Policies And Keeping The Big Data Monster At Bay: Legal Concerns In Healthcare In The Age Of The Internet Of Things

Christina Scelsi*

Care And Feeding Of Privacy Policies And Keeping The Big Data Monster At Bay: Legal Concerns In Healthcare In The Age Of The Internet Of Things

Christina Scelsi

Abstract

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right *to be let alone*. . .

KEYWORDS: Internet, healthcare, data

CARE AND FEEDING OF PRIVACY POLICIES AND KEEPING THE BIG DATA MONSTER AT BAY: LEGAL CONCERNS IN HEALTHCARE IN THE AGE OF THE INTERNET OF THINGS

CHRISTINA SCELSI*

* Christina Scelsi is the principal of Scelsi Entertainment and New Media Law with offices in Orlando and Port Charlotte, Florida, where she focuses her practice on entertainment, intellectual property, internet, technology, and business law. Ms. Scelsi has served as in-house counsel for an international game based-simulations company, where she was responsible for advising on software licensing matters, trademarks, copyright, and corporate issues. Ms. Scelsi began her practice in 2009, working with a punk music festival, and in years since has worked with clients ranging from software companies and independent filmmakers to professional daredevils and reality television participants. She is the Chair-Elect of the Florida Bar Entertainment, Arts and Sports Law Section. Ms. Scelsi has served as an editor of the book *Computer Games and Virtual Worlds: A New Frontier in Intellectual Property Law*, which was published by the ABA Section of Intellectual Property Law, is a chapter contributor to *The American Bar Association's Legal Guide to Video Game Development*, and is the author of the *PunkLawyer Blog*. Ms. Scelsi received her B.B.A. in marketing from Loyola University New Orleans, a J.D. from Saint Louis University School of Law, and an LL.M. in entertainment and media law from Southwestern School of Law.

I. INTRODUCTION

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right *to be let alone*. . . . [N]umerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[1]

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

The concept of privacy under the law, and concerns about invasion of that privacy in the face of new technologies is hardly new.[2] While the above quotation sounds like it could have come from a recent blog post or online news story, it is actually from the 1890 *Harvard Law Review* article *The Right to Privacy*, written by Supreme Court Justices Brandeis and Warren.[3] Though the article was inspired by the justices' concerns about the advent of snapshot photography that allowed reporters to take pictures of the justices and their families in public that were later published in the newspaper, when read amid today's concerns about privacy in the era of Google Glass and private drones, these concerns ring just as true as they did in the Nineteenth Century.[4] Technology company Cisco has estimated that ten billion devices were already connected to the Internet in 2013, and that this number will grow to more than fifty billion by 2020.[5] Of this growth, a recent Business Insider report estimates that enterprise use of the Internet of Things ("IoT") will lead at first, but that growth in the home and government sectors will ultimately surpass it, with government use of the IoT taking the lead by 2019.[6] This report also notes that experts believe the primary benefit of the growth of the IoT will be savings in terms of efficiency and costs for the home, government, and enterprise sectors; but that finding solutions to security and compatibility concerns related to the use of these devices is the key to enabling widespread adoption.[7] While technology continues to race ahead of the law, much remains unclear about how laws written in the age of paper records will apply to these new advances.[8] As the line between the user and the device becomes increasingly blurred, the need for legal and

2. *See id.* at 193–95.

3. *Id.* at 193, 220.

4. *See id.* at 195; Doug Gross, *This Gadget Can Knock Drones and Google Glass Offline*, CNN (Sept. 9, 2014, 10:41 AM), http://www.cnn.com/2014/09/08/tech/mobile/cyborg-unplug-google-glass/.

5. *See* Michael Endler, *Cisco CEO: We're All in on Internet of Everything*; INFORMATION WEEK (Feb. 25, 2013, 12:11 PM), http://www.informationweek.com/software/information-management/cisco-ceo-were-all-in-on-internet-of-everything/d/d-id/1108801?; FED. TRADE COMMISSION, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD i (2015), http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; *The Internet of Things*, CISCO, http://www.cisco.com/web/solutions/trends/iot/overview.html (last visited Aug. 20, 2015).

6. John Greenough, *The 'Internet of Things' Will Be the World's Most Massive Device Market and Save Companies Billions of Dollars*, BUS. INSIDER (Jan. 28, 2014, 8:35 AM), http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10.

7. *Id.*

8. *See* Warren & Brandeis, *supra* note 1, at 195, 199–200; FED. TRADE COMMISSION, *supra* note 5, at viii.

business privacy solutions that are agile and practical becomes even more paramount.[9]

While the use of big data that is generated by the IoT has great potential to produce boundless technological advances, it also presents some very real and serious legal concerns for consumers, as well as a number of regulated industries.[10] As these great changes occur, lawmakers and regulators will need to not only stay on top of the related need for updates and changes to the relevant laws—to protect consumers and businesses from the potential misdeeds that can be done using big data—but also be prepared to respond with effective solutions.[11] From the Target and Home Depot data breaches, to the dire possible results of the use of tools—like GPS spoofing devices that can take a plane or train off course, to the possible use of big data by terrorists, like was done in the Mumbai hotel attack of 2008—as the IoT develops, lawyers will be presented with challenges in the form of laws that are not up to date with the real world technologies that their clients are using, and opportunities to not only influence changes to these laws, but also to develop creative solutions to help clients navigate this changing landscape.[12]

A prime example of the myriad of data privacy issues that consumers and businesses face—both in regulated and unregulated industries—can be found in an examination of the issues currently faced by the healthcare industry in the age of the IoT.[13] While wearable fitness trackers, like FuelBand® and FitBit® devices, seem like innocuous gadgets urging users to move more and get in shape, the long term impact of having data about one's habits and health collected are unknown.[14] How would the data be viewed in the eyes of a person's physician, or insurance company for that matter?[15] When the device is more necessary for life—like a pacemaker capable of remote monitoring via the Internet—the implications of a data breach or potential attack by hackers become even more dire. When it comes to healthcare related applications, the Food and Drug Administration

9. *See* FED. TRADE COMMISSION, *supra* note 5, at 10.
10. *See id.* at 7–18.
11. *See id.*
12. *See* Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's; 'Unique, Custom-Built Malware' Eliminated from Retailer's Systems After Five-Month Attack on Terminals*, WALL ST. J. (Sept. 18, 2014, 5:43 PM), http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571; Marc Goodman, A Vision of Crimes in the Future, at TEDGlobal 2012 (June 2012), (transcript available at http://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future/transcript?language=en) [hereinafter Goodman, TEDGlobal 2012].
13. FED. TRADE COMMISSION, *supra* note 5, at 15–18.
14. *See id.* at 16.
15. *See id.* at 15–16.

("FDA") is considering different tiers of regulation to ensure that these apps are providing safe and accurate information to consumers.[16]

Health experts have expressed alarm at the safety and accuracy of health and fitness applications, or *apps*, prompting the FDA to investigate these apps, as well as propose new tiers of regulation to ensure that the information provided is safe and accurate.[17] This concern has proven to be well founded, as even the notoriously detail oriented technology company, Apple Computers, Inc., unveiled its new health data aggregation platform, HealthKit®, in a presentation featuring a slide that listed the user's blood glucose level erroneously as being measured in mL/dL, rather than in mg/dL.[18] In addition, a Federal Trade Commission ("FTC") examination of twelve health and fitness apps shared user data—such as names, email addresses, gender, as well as diet and fitness habits—with more than seventy-six third parties, a finding that is even more alarming when considered in conjunction with the reality that most of these apps do not feature privacy policies that disclose what data is collected, how it is used, and who it is shared with by the developer.[19]

When coupled with the push to convert medical records to electronic format as part of the implementation of the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"), and the rising problem of medical records identity theft, the importance of amending privacy laws like Health Insurance Portability & Accountability Act of 1996 ("HIPAA") to better protect patient data becomes all too clear.[20] As most privacy laws were drafted and enacted in the days of paper records, doing so

16. *See* Andrew Litt, *Caution: Untested mHealth Apps Proliferate, but Few Good Ones Work Well*, COMPUTERWORLD (Dec. 11, 2013, 6:00 AM), http://www.computerworld.com/article/2474276/healthcare-it/caution-untested-mhealth-apps-proliferate-but-few-good-ones-work-well.html; Amy Standen, *Sure You Can Track Your Health Data, But Can Your Doctor Use It?*, NPR (Jan. 19, 2015, 3:32 AM), http://www.npr.org/blogs/health/2015/01/19/377486437/sure-you-can-track-your-health-data-but-can-your-doctor-use-it.

17. Mark Sullivan, *Apple's On-Stage Healthkit Goof Proves It Still Has to Earn the Trust of the Health Community*, VENTUREBEAT (June 4, 2014, 6:10 AM), http://venturebeat.com/2014/06/04/apples-on-stage-healthkit-goof-proves-it-still-has-to-earn-the-trust-of-the-health-community/; Elizabeth Weise, *FDA Sets Guidelines for Medical Devices' Cybersecurity*, USA TODAY (Oct. 1, 2014, 4:32 PM), http://www.usatoday.com/story/tech/2014/10/01/fda-medical-devices-cybersecurity/16543731/.

18. Sullivan, *supra* note 17.

19. *See* Christina Farr, *FTC Commissioner Warns on Mobile Health-Data Gathering*, REUTERS (July 23, 2014, 8:52 PM), http://www.reuters.com/article/2014/07/24/us-healthcare-tech-washington-idUSKBN0FT02320140724.

20. *See* Health Information Technology for Economic & Clinical Health Act of 2009, Pub. L. No. 111–5, § 13001, 123 Stat. 226, 226; Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104–191, § 1, 110 Stat. 1936, 1936.

will not only involve the input of lawmakers, but also of the creators of the affected technologies.[21]

II. WHAT IS THE INTERNET OF THINGS?

A. *Definition*

The IoT is defined by the FTC as:

> [T]he ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day.[22]

The FTC estimates that this trend is only still in its infancy, stating that experts estimate that as of 2015, there will be twenty-five billion connected devices, and by 2020, there will be more than fifty billion such connected devices.[23] In its summary of the workshop titled *The Internet of Things: Privacy and Security in a Connected World*, the FTC notes the many benefits presented by the IoT, such as how "connected medical devices can allow consumers with serious medical conditions to work with their physicians to manage their diseases."[24] However, the FTC also notes that the IoT presents "security risks [to consumers] that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety."[25]

The FTC report states that the principles that it is basing its recommendations on for the IoT are the Fair Information Practice Principles of "notice, choice, access, accuracy, data minimization, security, and accountability."[26] The principle of data minimization refers to the idea that companies "should limit the data [that] they collect and retain, and

21. Jason Wang, *HIPAA Compliance: What Every Developer Should Know*, INFORMATIONWEEK (July 11, 2014, 9:06 AM), http://www.informationweek.com/healthcare/security-and-pray/hipaa-compliance-what-every-developer-should-know/a/d-id/1297180; *see also* FED. TRADE COMMISSION, *supra* note 5, at ii.

22. FED. TRADE COMMISSION, *supra* note 5, at i.

23. *Id.*

24. *Id.* at i–ii.

25. *Id.* at ii.

26. *Id.*

[ultimately] dispose of it once" the data is no longer needed.[27] The report notes that there was division among the participants in regard to this principle, as some participants expressed concern that "requiring fledgling companies to predict what data they should minimize would 'chok[e] off potential benefits and innovation.'"[28] The participants in the workshop also noted that one of the challenges with the IoT is providing notice to the user that the device is collecting data.[29]

There was also some division as to the principles of notice and choice among the workshop participants, based in large part upon the ubiquity of these devices.[30]

> As one participant observed, [if consumers have] "a bunch of different sensors on a bunch of different devices, on your home, your car, your body . . . measuring all sorts of things" it would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported.[31]

The major concern among participants as it relates to the risk is if patients are faced with too many requests for consent to the collection of data, they will stop using the device, which could be a serious problem in the case of medical IoT devices.[32] The participants found this to be especially true with medical devices that have no screen or other interface that would enable it to communicate said notice to the user, or in the case of devices with screens, they are smaller than the screens on mobile devices and make it difficult, if not impossible, to communicate the notice to the user.[33] The timing of the request may also be an issue that prevents users from reading a notice, let alone consenting to it, such as when a consumer may be driving.[34]

B. *Prediction of Impact*

There is no doubt that the IoT will affect nearly every industry, whether in terms of better planning as a result of the analysis of data collected by smart devices, or in the increased efficiencies created by the ability for people to use devices to communicate data to people located

27. FED. TRADE COMMISSION, *supra* note 5, at iv.
28. *Id.* at 21 (alteration in original).
29. *Id.* at v.
30. *Id.*
31. *Id.* at 22.
32. FED. TRADE COMMISSION, *supra* note 5, at v.
33. *Id.* at 22.
34. *Id.*

remotely.[35] Just in the healthcare industry, remote monitoring of patients over the Internet estimated to reduce hospital visits by forty percent and cost per visit by $1800 for implantable medical devices.[36]

For the purposes of this Article, the focus will be on the potential impacts of IoT and the data collected by these devices on the healthcare industry.[37]

C. *Data*

1. How Data is Collected in Healthcare

The healthcare industry is particularly unique in terms of the IoT in that it has perhaps the largest variety of types of data that can be collected, as well as devices to collect it.[38] From blood pressure levels to levels of different materials in blood to oxygen saturation—among many others—healthcare professionals can monitor what is going on with a patient from head to toe.[39] In addition, there are numerous conditions that can be monitored, and just as many types of devices to monitor them.[40]

2. How Data is Used in Healthcare

Medical data is used for a number of purposes, including for patient diagnosis and treatment.[41] In addition, this same information can be shared with insurance companies for billing purposes, government agencies collecting data, research institutions and organizations, prevention and wellness initiatives, and for the education of health care providers, patients, families, communities, government, and other organizations.[42]

---

35. *See id.* at 7–8.

36. Gregor Koenig, Barracuda Networks AG, Security and Privacy of Wireless Implantable Medical Devices 4, Presentation at Security Forum 2013 (Apr. 17, 2013).

37. *See infra* Part II.C–D.

38. DARRELL M. WEST, CTR. FOR TECH. INNOVATION AT BROOKINGS, IMPROVING HEALTH CARE THROUGH MOBILE MEDICAL DEVICES AND SENSORS 1–4, 8 (2013).

39. *See id.* at 1, 8.

40. *See id.* at 1–4.

41. *See* Andy Ferris et al., *Big Data: What Is It, How Is It Collected and How Might Life Insurers Use It?*, ACTUARY, Dec. 2013–Jan. 2014, at 28, 30; WEST, *supra* note 38, at 1, 3–4.

42. *See* Ferris et al., *supra* note 41, at 29–30.

D. *Crime Concerns*

1. General and Healthcare Related Crime Concerns

While there are great expectations as to what solutions the advent of big data will bring to various industries and to consumers, there are also equally large concerns about how such data could be used by those with nefarious intent.[43] Marc Goodman of the Future Crimes Institute has spoken about the future of crime in the age of big data, and the picture so far is not pretty.[44] While the data breaches at Target and Home Depot in 2014 caused consumers financial headaches, the potential of criminal activity in the future according to Goodman could be far worse.[45] As Goodman notes, going back to the time of Neanderthals, data has been a double sided coin with both good and bad aspects; and in today's environment of three-dimensional printing and other high tech weapons, where the positive aspects have great potential, the negative present consequences will call for regulatory solutions in coming years.[46] The primary example that he cites in his TED talk is the 2008 terrorist attack on a hotel in Mumbai.[47] What marked a shift from previous such attacks was that, while these terrorists attacked with the expected weapons of hand grenades, explosives and machine guns, they also came armed with mobile phones, night vision goggles, access to satellite imagery, and most importantly, access to an operations center in Pakistan.[48]

The terrorist operations center allowed the people working there to monitor mainstream media coverage of the attack on television channels like CNN, the BBC, Al-Jazeera, and local Indian television stations, as well as the internet, and most importantly, social media.[49] It was these latter sources that made the Mumbai attack so different from previous terrorist attacks; as the terrorists were able to call the war room as they moved through the hotel to have their operatives google the hostages and search social media to find out information about them that helped the terrorists gain advantages in their negotiations.[50] In one such instance, the terrorists were able to learn that a hostage who claimed to be a schoolteacher was actually the second-wealthiest businessman in India, and after this information was revealed, the

43. *See What Does the Future of Crime Look Like?*, NPR (Sept. 13, 2013, 9:39 AM), http://www.npr.org/templates/transcript.php?storyId=215831944.
44. *Id.*
45. Sidel, *supra* note 12; *What Does the Future of Crime Look Like?*, *supra* note 43.
46. *See What Does the Future of Crime Look Like?*, *supra* note 43.
47. Goodman, TEDGlobal 2012, *supra* note 12.
48. *Id.*
49. *Id.*
50. *Id.*

terrorists in the operations center gave the order to the terrorists on the ground to kill the man.[51] Goodman sums up the impact of the situation, and the enhanced ability on the part of the terrorists to create such terror:

> Think about what happened. During this [sixty]-hour siege on Mumbai, [ten] men armed not just with weapons, but with technology, were able to bring a city of [twenty] million people to a standstill. Ten people brought [twenty] million people to a standstill, and this traveled around the world. This is what radicals can do with openness.[52]

The Internet is also cited as not only a means of providing information about hostages, but also to commit massive crimes, such as the hack of the Sony PlayStation Network, which resulted in the robbery of one hundred million people in one fell swoop.[53] Goodman notes in his talk how every advance in technology—from drones to three-dimensional printing—can be used not only for good, but also for evil by criminals.[54] Three-dimensional printing is certainly a prime example of this, for while the technology can and has been used by doctors to create prosthetic body parts to save lives, it has also been used to create weapons.[55] While these weapons have yet to be used by criminals to commit crimes, there has been concern on the part of lawmakers and law enforcement that the ability to print these weapons from non-metal materials could be used to smuggle said weapons through security checkpoints and on to planes, or into other sensitive areas to carry out terrorist attacks.[56] Goodman has also written about the *Big Brother* aspect of big data where implantable medical device data could be used as part of an autopsy to determine a person's cause of death.[57]

This concern about the potential nefarious use of new devices and the associated data collected by them becomes even graver when one considers the implications of a data breach of health devices.[58] While devices like cochlear implants, diabetic pumps, pacemakers, and defibrillators have changed lives for thousands of people, it is important to remember that these very devices are also collecting and transmitting data

51. *Id.*
52. Goodman, TEDGlobal 2012, *supra* note 12.
53. *Id.*
54. *Id.*
55. *See id.*
56. *See id.*
57. *See* Marc Goodman, Future Crimes Inst., Who Does the Autopsy? Criminal Implications of Implantable Medical Devices 3, Presentation at the 2nd USENIX Workshop on Health Security and Privacy (Aug. 9, 2011); Koenig, *supra* note 36, at 20.
58. Goodman, *supra* note 57, at 2.

about the patients in which they have been implanted.[59] Goodman uses pacemakers as an example, noting that sixty thousand people in the United States have a pacemaker that connects to the Internet and allows a physician to shock the heart remotely in the event that the patient needs it.[60] In the hands of the physician, it could be a lifesaver, but in the hands of a criminal, the ability to shock the patient remotely could be a means of committing murder.[61] While these pacemakers represent a small fraction of all the devices that have been implanted, the connected devices are estimated to increase in terms of adoption, hence the concern about the impact of that increase in usage, as well as the potential need to update older models to these newer IoT models.[62]

Even in the case of less crucial devices like fitness trackers such as Fitbit® or FuelBand®, the data collected from these devices has already been admitted as evidence in a personal injury trial in Calgary in 2014.[63] This case is even more significant, as the attorneys are not just using the data from the Fitbit®, but are instead putting it through an analytics platform that "uses public research [data] to compare [the] person's activity data with that of the general [public]."[64] Couple this data with information that can be discovered from social media, and the concern that wearable technology like fitness trackers could become like *black boxes* for humans, seem to be becoming all too real.[65]

It is scenarios like those discussed above that led the FDA and the Department of Homeland Security to focus their attention on finding solutions to the potential risks presented by the IoT as it relates to healthcare.[66] In addition to proposing the regulations that will be discussed later in this paper, the leaders of the FDA have made it widely known that they will be keeping an eye on developers of apps and devices designed for this market.[67] Shortly before the guidelines were introduced in October of

59. FED. TRADE COMMISSION, *supra* note 5, at 16; Goodman, TEDGlobal 2012, *supra* note 12.

60. Goodman, TEDGlobal 2012, *supra* note 12.

61. *See id.*

62. Sue Poremba, *A Movement Is Needed to Improve Cyber Security for Medical Devices*, SUNGARD AVAILABILITY SERVICES (Jan. 23, 2015), http://blog.sungardas.com/2015/01/a-movement-is-needed-to-improve-cyber-security-for-medical-devices/#sthash.C6JIT9KN.dpbs.

63. *See, e.g.*, Parmy Olson, *Fitbit Data Now Being Used in the Courtroom*, FORBES (Nov. 16, 2014, 4:10 PM), http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/.

64. *Id.*

65. *See id.*

66. Poremba, *supra* note 62.

67. FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (2015), *available at* http://

2014, Suzanne Schwartz, the director of emergency preparedness at the FDA's Center for Devices and Radiological Health, stated that "[t]here is no such thing as a threat-proof medical device," and "[i]t is important for medical device manufacturers to remain vigilant about cybersecurity and to appropriately protect patients from those risks."[68] The FDA has been emphatic in urging developers and manufacturers to think about security in developing new products, and to anticipate potential solutions before releasing them to the marketplace.[69] Chief among the considerations that developers and manufacturers should keep in mind during development are, "[a]t a minimum, medical devices should require secure authentication for access, use encrypted communication, and make sure that security patches are always added."[70]

While the FDA has released regulations to help with the current and future apps and devices that will be developed as part of the healthcare IoT, there are also unique challenges presented by the older medical devices as technology develops around them.[71] The fact of the matter is that these older devices present their own security threat, for reasons varying from that the software used for these devices is not able to be patched, or that they were never tested for security flaws.[72] Further, in the case of implantable medical devices, the challenges rise to a whole new level, as updating them can involve surgery, making it not only a conversation about improving patient data security, but also a decision between a patient and his or her physician as to whether such surgery is best for the patient from a medical perspective.[73] This adds another piece to an already complicated puzzle for physicians, who must now not only consider the potential medical benefit to the patient presented by implanting a medical device, but also the long-term maintenance requirements presented by it.[74] This is where physician education by representatives from medical device companies will play a crucial role in helping physicians navigate these considerations so that they can then help patients make these decisions.[75]

---

www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

68. Weise, *supra* note 17.
69. *Id.*
70. *Id.*
71. Poremba, *supra* note 62.
72. *Id.*
73. *Id.*
74. *Id.*
75. *See id.*

i. *Hypothetical: Hacking an Insulin Pump*

Perhaps the best deep dive into the potential ways in which a smart medical device or application could be hacked for criminal purposes is the 2011 talk by Jerome Radcliffe at the Black Hat cyber security conference.[76] Radcliffe, a diabetic man, spoke about his experiments into how one might hack his insulin pump.[77] His talk started with what would seem to be the most obvious source of information about the communication systems that the pump uses: The user manual.[78] He noted how the appendix of the user manual provided him with everything from the wireless frequency on which it operated to how often information was sent, and how large the file sizes were.[79] Radcliffe also learned the Federal Communications Commission ("FCC") identification number from the manual, which he then took to the FCC website, where a simple search resulted in downloadable FCC verification documents for the device that detailed the process by which the pump transmits data to the continuous glucose monitor ("CGM").[80]

With this information acquired, Radcliffe moved on to considering the types of hacks that a hacker could carry out on an insulin pump user.[81] He notes that perhaps the most dangerous type of attack would be a spoofing attack that would manipulate the sensor data that could lead an unsuspecting user to think that his or her sugar levels are higher or lower than they actually are.[82] However, Radcliffe goes on to explain that while such a hack would be possible, there are characteristics of how the pump and its components work that would make carrying out such a hack difficult.[83] First, the range of the CGM receiver is very limited, meaning that the transmitter would need to be within one hundred to two hundred feet of the receiver in order to work.[84] Second, if such a reading was detected by the pump, the device would require the user to calibrate it using a blood glucose meter, the intervention of which would be highly unlikely.[85] Finally, Radcliffe explains that even if a criminal was able to manipulate the user into administering too much

76. Jerome Radcliffe, Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System at Black Hat USA 2011 (Aug. 3–4, 2011), *available at* https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf.

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

81. Radcliffe, *supra* note 76.

82. *Id.*

83. *Id.*

84. *Id.*

85. *Id.*

insulin, it is not uncommon for diabetics to experience such levels, meaning that the hacker would need to continue manipulating the sensor data for hours to keep impacting the user, a fact that makes it unlikely such an attack would be successful.[86]

Radcliffe goes on to examine the likelihood of the success of carrying out such an attack using the wireless communication functions of the insulin pump.[87] He states that a particularly dangerous situation for a diabetes insulin pump user would be when—unbeknownst to the user—the configuration settings that are the basis for calculating the amount of insulin that is to be dispensed have been manipulated.[88] He posits that this type of attack would likely involve using the wireless peripheral device that is necessary to talk to the pump, a task that is made relatively simple due to the availability of the device for sale on the Internet, and the publication of the command codes online.[89] With the device and command codes in hand, Radcliffe estimates that a hacker could change the configuration settings in a short amount of time, and for example, could change the setting controlling the ratio of insulin given at meal time enough to cause a diabetic patient to become hypoglycemic within sixty to ninety minutes after eating.[90] However, as with the CGM devices, Radcliffe explains that the likelihood that such an attack would succeed are limited by several factors.[91] He starts by noting that like the CGM devices, the wireless components in the pump have a very limited range of only one hundred to two hundred feet.[92] The most significant limiting factor for the success of a wireless attack is the fact that the attacker would need the serial number of the device, which could not be obtained without physical access to the device.[93]

The exploration of the potential hacking of an insulin pump concludes as Radcliffe observes that perhaps the most dangerous element of the medication delivery process for diabetic patients is that presented by humans in the form of the manipulation of the variables used to determine the amount of insulin to be given.[94] However, he points to the trend of trying to remove the risk of human intervention from the equation that is currently leading organizations like the Juvenile Diabetes Research Foundation to explore computer-operated insulin delivery options through its *Artificial*

86. Radcliffe, *supra* note 76.
87. *See id.*
88. *Id.*
89. *Id.*
90. *Id.*
91. *See* Radcliffe, *supra* note 76.
92. *Id.*
93. *Id.*
94. *Id.*

Pancreas Project.[95] While such solutions would eliminate the risk of human intervention, Radcliffe remarks that these new automated solutions may reduce or eliminate one type of risk, but also present new risks that may be greater in the attack scenarios that he had considered—as such attacks would be on an automated system—and less human intervention would also mean less human oversight to detect them.[96]

2. Data Discrimination

In addition to concerns about actual physical harm caused by hacks or malfunctions by smart devices, perhaps the other greatest concern is that of discrimination on the basis of the data collected by these same devices.[97]

While there are many issues related to the growth of the IoT and the data collected by the devices in its ecosystem, this Article focuses on the legal implications of the IoT as it relates to healthcare devices.[98] Much like the potential hacking of a lifesaving device, it is not entirely unthinkable that Uber data could be used to make determinations in relation to whether a person is accepted for housing, or that health insurance companies could try to access policy holders' credit card purchase data to inspect it for alcohol or tobacco purchases—or medical marijuana for that matter—and deny coverage based on data showing activities by policy holders that it finds unacceptable.[99] Or, imagine if the data collected by health devices and apps—as to whether policy holders are properly managing their health conditions—were to be used as the basis to find the person to be non-compliant and perhaps deny coverage, or even to make employment decisions.[100]

E. *Internet of Things and Health Devices*

One of the fastest growing sectors of the IoT is that related to health care devices and apps.[101] The Intel's report to the Senate Special Committee on Aging estimates that "[i]n large part because of widespread wastefulness in service delivery and need for virtual care models, McKinsey forecasts that

95. *Id.*
96. Radcliffe, *supra* note 76.
97. *See id.*; U.S. Dep't of Health & Human Servs., *Health Information Privacy: Genetic Information*, www.hhs.gov/ocr/privacy/hipaa/understanding/special/genetic/index.html (last visited Aug. 20, 2015).
98. *See infra* Part III.
99. *See* FED. TRADE COMMISSION, *supra* note 5, at 14–17; Radcliffe, *supra* note 76.
100. *See* FED. TRADE COMMISSION, *supra* note 5, at 15–16.
101. *Id.* at 3.

[forty] percent of the global economic impact of the IoT revolution will occur in healthcare, more than any other sector."[102] What began with simple heart rate monitors and fitness trackers has now given way to devices that can take photographs and videos of the inner ear and transmit them to a remotely located physician, allowing him or her to diagnose an ear infection using a smartphone.[103] Researchers have even developed a temporary tattoo with electrodes that use a mild electrical current to monitor the wearer's blood sugar levels.[104]

Why is there so much interest and growth in terms of IoT smart devices and apps for healthcare? A presentation at the Senate Special Committee on Aging cites a number of reasons for it:

- a previously unseen aging population, in which "[t]here will be more people over age [sixty-five] than under age [five];"
- an increase in chronic diseases;
- "[g]lobal shortage of healthcare workers;"
- a dramatically inefficient healthcare sector;
- "a shift from passive to active patients;" and
- rapid growth of health apps, social networks, and collaboration tools.[105]

As part of the growth of IoT in healthcare, the presentation notes three emerging categories: (i) person to person; (ii) person to computer; and (iii) person as computer.[106]

F. *Policy and Security Recommendations*

As one can imagine, for as much interest as there is in developing apps and devices for the healthcare sector, there is just as much or even more interest in developing solutions to keep healthcare data safe.[107] The recent

---

102. INTEL, THE INTERNET OF THINGS AND HEALTHCARE POLICY PRINCIPLES 1 (2014), *available at* http://www.aging.senate.gov/imo/media/doc/Intel%20-%20IoT-Healthcare%20Policy%20Principles%20FINAL%207-25-14%20%20(3).pdf.

103. *See* Standen, *supra* note 16; Eliza Strickland, *Diagnosing Ear Infections With a New Smartphone Gadget*, IEEE SPECTRUM (Dec. 15, 2014, 14:00 GMT), http://www.spectrum.ieee.org/tech-talk/biomedical/devices/diagnosing-ear-infections-with-a-new-smartphone-gadget-.

104. Robert Ferris, *A 'Tattoo' May End Fingerpricks for Diabetics*, CNBC (Jan. 15, 2015, 11:56 AM), http://www.cnbc.com/id/102337534.

105. INTEL, *supra* note 102, at 1–2.

106. *Id.* at 3.

107. *See Examples of MMAs the FDA Regulates*, U.S. FOOD AND DRUG ADMIN., http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm368743.htm (last updated July 15, 2015); INTEL, *supra* note 102, at 4; Anna Wilde Matthews & Danny Yadron, *Health Insurer Anthem Hit by*

data breach at Anthem Inc.—the second largest health insurer in the United States—involved "hackers br[eaking] into a database containing [the] personal information [of] about [eighty] million of its customers and employees."[108] This hack is estimated "to be the largest data breach [that has been] disclosed by a healthcare company" to date, and demonstrates the great risk that companies handling healthcare data face in terms of data breaches due to hacker attacks, lost computers or hard drives, and other methods.[109] Even though the breach thus far seems to be limited to the names, birthdays and addresses of customers and employees, it is still estimated that *tens of millions* of records were stolen, and it still represents a massive incursion for the company and for consumers.[110]

Given the very real risk of data breaches, regulatory agencies—as well as federal and state legislatures—are keeping an eye on the situation and are recommending security guidelines for the IoT as it relates to healthcare.[111] Intel presented to the Senate Special Committee on Aging recommendations for policies related to the development of security measures for healthcare data.[112] The first policy principle posited by the Committee is to require data standards for connectivity, as well as for interoperability between smart devices.[113] As the Committee's report on the IoT notes, "[the] IoT in healthcare has the potential to aggregate data from patient records, wearable sensors, labs, diet, the environment, and social networking in real time, but only if the data can be analyzed. This takes standardized data formats."[114] The second policy principle for securing the IoT for healthcare put forth by the Committee is to regulate smartly, and avoid *de-innovation* in developing security standards.[115] The report emphasizes the need for collaboration between the relevant parties, such as

---

Hackers: Breach Gets Away with Names, Social Security Numbers of Customers, Employees, WALL ST. J. (Feb. 4, 2015, 9:39 PM) http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720; Michelle McNickle, *6 Best Ways to Protect Against Health Data Breaches*, HEALTHCARE IT NEWS (Sept. 30, 2011), http://www.healthcareitnews.com/news/6-best-ways-protect-against-health-data-breaches?single-page=true.

108. Matthews & Yardon, *supra* note 107.

109. *Id.*; *see also* Richard W. Walker, *Negligent Employees Cause Most Data Breaches; Mobile is Key Factor*, BREAKING GOV'T (Mar. 22, 2012, 1:32 PM), http://www.breakinggov.com/2012/03/22/negligent-employees-cause-most-data-breaches-mobile-is-key-fact/.

110. Matthews & Yardon, *supra* note 107.

111. *See id.*; INTEL, *supra* note 102, at 3–4.

112. INTEL, *supra* note 102, at 3.

113. *Id.*

114. *Id.*

115. *Id.* at 3–4.

has been done by the Congress, regulators, and industry to develop regulatory frameworks like the FDA Safety Innovation Act.[116]

The third policy principle noted in Intel's report to the Senate Special Committee on Aging for the IoT for healthcare is rethinking reimbursement.[117] The discussion of this principle notes that much of the "rich and actionable data is not being used today because our health systems are unprepared to incorporate the data into the fee for service payments, or shared savings models."[118] The report cites how the adoption of virtual care for patients by physicians and healthcare systems has been delayed thus far, not by technology, but by the fact that providers are not paid for situations where such virtual care is substituted and enhanced over in person visits.[119] The next policy principle that the Committee report emphasizes is to capture patient generated health data as a vital part of the patient record.[120] It is stated in the report how the twenty-seven billion dollar investment made by the U.S. Government in promoting the adoption of electronic medical records through the HITECH Act resulted in "unparalleled adoption rates—[seventy-eight] percent of physicians and [sixty-six] percent of our nation's qualifying hospitals have been certified. Yet, the real time data from sensors, tablets, smartphones, and peripherals are not captured in the [electronic health records]."[121]

The final security policy recommendation included in Intel's report to the Committee is that privacy and security standards be required for IoT applications and devices that are part of the IoT.[122] As the report states, according to the Office for Civil Rights in the Department of Health and Human Services ("HHS"), "199 [personal health information] ("PHI") breaches were reported in 2013, affecting [seven] million patient records."[123] It urges HHS to continue its efforts to work with interested parties to find a "universally accepted health IT security standard or [principles] that can be enforceable and agree on criteria that deems organizations 'HIPAA Security Rule Compliant.'"[124]

116. *Id.*
117. INTEL, *supra* note 102, at 4.
118. *Id.*
119. *Id.*
120. *Id.*
121. *Id.*
122. INTEL, *supra* note 102, at 4.
123. *Id.*
124. *Id.*

III. LEGAL ASPECTS OF THE INTERNET OF THINGS

A. *General Data*

There are a number of legal aspects in play when it comes to big data, both in terms of more general privacy laws, as well as laws specific to certain types of data, such as medical records.[125] What has become particularly interesting as the Internet and the IoT have developed, is the interplay of the obligations imposed by the various privacy laws upon new parties who likely did not initially anticipate being subject to them, such as web developers who take on a project for a school system and find themselves subject to the requirements of Family Education Rights and Privacy Act or Children's Online Privacy Protection Act ("COPPA"), or an app developer with an idea for a healthcare application that finds himself or herself subject to HIPAA and FDA regulation.[126] As such, it has become more important than ever that web developers and information technology professionals working with healthcare clients are not only aware of the requirements of these laws, but can also help their clients find effective compliance solutions. Privacy policies for websites and software that collect data have become a cornerstone of this process, as they not only allow the website operator to communicate its privacy policies and processes to users, but also to demonstrate its commitment to compliance to regulators. These privacy policies are unique, living documents that, just like the magical creatures that Harry Potter and his friends at Hogwarts had to learn about in their Care and Feeding of Magical Creatures class, require proper care and feeding to thrive.

1. Federal Privacy Act of 1974

The Privacy Act of 1974 governs the collection, maintenance, use, and dissemination of information about individuals that is stored in the records systems of federal agencies.[127] The Act defines a system of records as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[128] It further establishes the no disclosure without consent rule, which states "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency,

125. *See infra* Part III.A–C.
126. *See infra* Part III.A.2–3, B.4, C.3.
127. 5 U.S.C. § 552a(e) (2012).
128. *Id.* § 552a(a)(5).

except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[129] This rule is subject to twelve exceptions, ranging from an agency's need to know the information, to responding to Freedom of Information Act requests, to responding to court orders.[130]

The Privacy Act grants the following rights to people: To find out what information was collected about them; to see and have a copy of that information; to correct or amend that information; and to exercise limited control of the disclosure of that information to other parties.[131]

The Privacy Act comes into play for healthcare organizations that are operated by the federal government, such as the Veterans' Health Administration, as well as record systems operated as part of a contract with a federal government agency.[132]

2. COPPA

One privacy law that has been in the spotlight in recent years due to enforcement actions by the FTC is the COPPA.[133] Passed in 1998, this law protects the personally identifiable information ("PII") of children under the age of thirteen and sets out regulations that commercial website operators must abide by if the website is collecting such information.[134] The law defines personal information to include: "[F]irst and last name; [a] home or other physical address, including street name and name of a city or town; [o]nline contact information; . . . a screen or user name [that] functions . . . as online contact information; . . . [a] telephone number; [and a] social security number."[135]

COPPA prohibits operators of commercial websites from collecting or disclosing the personal information of minors under the age of thirteen without verifiable parental consent.[136] The law not only requires website operators to put mechanisms in place to comply with COPPA but also to provide notice to parents about what information is collected by the site and how that information will be used, even if the parents consent.[137] COPPA applies even if the website is not targeted specifically at children.[138] So long

129. *Id.* § 552a(b).
130. *Id.* § 552a(b)(1)–(12).
131. *See id.* § 552a(b)–(e).
132. *See* 5 U.S.C. § 552a(f).
133. 16 C.F.R. §§ 312.1–.12 (2014).
134. *Id.* §§ 312.1–.2.
135. *Id.* § 312.2.
136. *Id.* § 312.3.
137. *Id.* §§ 312.3–.4.
138. *See* 16 C.F.R. § 312.3.

as the website is collecting PII from children, it must be in compliance with the law.[139] This is why many commercial websites that allow users to register either require users to check a box certifying that they are over the age of thirteen or do not permit users under the age of thirteen to register.[140]

The FTC announced revisions to COPPA in 2013.[141] These changes included an expansion of the definition of what was considered personal information to include:

- A "*persistent identifier*[] that can be used to recognize [a] user[] over time and across . . . websites or online services," such as cookies, IP addresses, and mobile device IDs;[142]
- A photograph, video, or audio file, where such file "contain[s] a child's image or voice";[143]
- Geolocation information sufficient to identify street name and name or a city or town;[144] and
- Information concerning the child or the parents of that child that the operator combines with an identifier described above.[145]

The FTC's amendments to the COPPA rules in 2013 also expanded the definition of a commercial website *operator* to include not only the operator of a website or service directed at children, but also of "outside services, such as plug-ins or advertising networks that collect personal information from . . . visitors."[146] The amendments also clarified that COPPA applies to "plug-ins or ad networks that have actual knowledge that

139. *Id.*

140. *See id.*

141. Press Release, Fed. Trade Comm'n, FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information by Protection Rule (Dec. 19, 2012), http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over; *see also* 16 C.F.R. § 312.

142. Press Release, Fed. Trade. Comm'n, *supra* note 141. *Compare* 16 C.F.R. § 312.2 (2012) *with id.* § 312.2 (*Personal Information*) (2014).

143. Press Release, Fed. Trade. Comm'n, *supra* note 141. *Compare* 16 C.F.R. § 312.2 (2012) *with id.* § 312.2 (*Personal Information*) (2014).

144. Press Release, Fed. Trade. Comm'n, *supra* note 141. *Compare* 16 C.F.R. § 312.2 (2012) *with id.* § 312.2 (*Personal Information*) (2014).

145. Press Release, Fed. Trade. Comm'n, *supra* note 141. *Compare* 16 C.F.R. § 312.2 (2012) *with id.* § 312.2 (*Personal Information*) (2014).

146. Press Release, Fed. Trade. Comm'n, *supra* note 141; *see also Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMMISSION, http://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Questions (last updated Mar. 20, 2015). *Compare* 16 C.F.R. § 312.2 (2012) *with id.* § 312.2 (*Personal Information*) (2014).

they are collecting personal information through a . . . website or online service" directed at children.[147]

In updating COPPA, the FTC aimed to streamline and clarify the requirements for direct notice to parents in such a way that it ensures that the information is provided to parents in a succinct manner that provides this information *just in time*.[148] The Commission also expanded the list of acceptable methods for operators to obtain prior verifiable parental consent from parents, created new exceptions to the rule's notice and consent requirements, and strengthened the data security protections.[149] The amendments also require that operators have reasonable data retention and deletion procedures.[150] As part of the new changes, the FTC strengthened its oversight of the self-regulatory safe harbor programs, and instituted a "voluntary pre-approval mechanism[] for new [methods of consent]," as well as "for activities that support the internal operations of a website or online service."[151]

The FTC initially granted website operators a grace period during which it would allow operators a chance to update their procedures to meet the requirements of the new amendments, but in 2014, it started enforcing the new regulations.[152] Among the notable settlements was a $450,000 settlement with the online review website Yelp for not having the proper COPPA compliance mechanisms in place as part of its mobile app.[153] The irony of the settlement—as noted by the FTC in its press release—was that Yelp had the appropriate mechanisms in place on its full website, just not on the mobile app.[154]

147. Press Release, Fed. Trade. Comm'n, *supra* note 141; *see also Complying with COPPA: Frequently Asked Questions*, *supra* note 146. *Compare* 16 C.F.R. § 312.2 (2012) *with id.* § 312.2 (*Personal Information*) (2014).

148. *Complying with COPPA: Frequently Asked Questions*, *supra* note 146; Press Release, Fed. Trade. Comm'n, *supra* note 141; *see also* 16 C.F.R. § 312.4 (2014).

149. 16 C.F.R. § 312.5–.8; *Complying with COPPA: Frequently Asked Questions*, *supra* note 146; Press Release, Fed. Trade Comm'n, *supra* note 141.

150. 16 C.F.R. § 312.10; *Complying with COPPA: Frequently Asked Questions*, *supra* note 146.

151. *Complying with COPPA: Frequently Asked Questions*, *supra* note 146; *see also* 16 C.F.R. § 312.5; Press Release, Fed. Trade Comm'n, *supra* note 141.

152. Lesley Fair, *Updated FAQs to Help Keep Your Company COPPA-Compliant*, FED. TRADE COMMISSION (Apr. 25, 2013, 11:22 AM), http://www.ftc.gov/news-events/blogs/business-blog/2013/04/updated-faqs-help-keep-your-company-coppa-compliant; Press Release, Fed. Trade Comm'n, Yelp, TinyCo Settle FTC Charges Their Apps Improperly Collected Children's Personal Information (Sept. 17, 2014), http://www.ftc.gov/news-events/press-releases/2014/09/yelp-tinyco-settle-ftc-charges-their-apps-improperly-collected.

153. Press Release, Fed. Trade Comm'n, *supra* note 152; *see also* 16 C.F.R. §§ 312.3–.5.

154. *See* Press Release, Fed. Trade Comm'n, *supra* note 152.

While COPPA is not a law that addresses health care directly, the FTC has said in a recent report that it is among the laws that it intends to use to police the IoT as it develops.[155] Given the unprecedented use of Internet-connected devices by children in recent years, it is likely that there will need to be further amendments made to COPPA by the FTC to include the ever-evolving categories of data collected by them.[156]

3. California Online Privacy Protection Act ("CalOPPA")

In addition to the federal efforts to protect Internet users online, states have also been implementing their own laws to protect their citizens on the Internet.[157] Perhaps the most significant such state law is CalOPPA.[158] This law requires all commercial operators of websites or online services to conspicuously post privacy policies to inform consumers about: (a) the categories of PII being collected; and (b) with which third parties the PII will be shared.[159]

California introduced amendments to CalOPPA that took effect on January 1, 2015.[160] Among these amendments was a requirement that retail website operators include a *delete button* on such sites and applications that would allow minors who are registered users on the site to have the ability to delete their content that has been posted on the site, or the ability to request that it be deleted.[161] These amendments also require that operators provide notice that they have the ability to delete online content and instructions on how to do so.[162] Finally, the amendments prohibit retail website operators from advertising certain categories of products or services to minors.[163] It is worth noting that the operators of the major app platforms have entered into

155. Lesley Fair, *Internet of Things: FTC Staff Report and a New Publication for Business,* FED. TRADE COMMISSION (Jan. 27, 2015, 9:12 AM), http://www.ftc.gov/news-events/blogs/business-blog/2015/01/internet-things-ftc-staff-report-new-publication-businesses; *see also* 16 C.F.R. §§ 312.1–.12.

156. *See* Fair, *supra* note 155.

157. *See, e.g.*, CAL. BUS & PROF. CODE §§ 22575–79 (West 2014).

158. *See id.*; KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, MAKING YOUR PRIVACY PRACTICES PUBLIC 5 (2014), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

159. CAL. BUS. & PROF. CODE § 22575(a)–(b)(1).

160. *See id.* §§ 22580–82.

161. *Id.* § 22581(a)(1); Gregory T. Parks et al., *California's "Delete Button" Law Re: California Online Privacy Protection Act (CalOPPA)*, NAT'L L. REV. (Oct. 16, 2013), http://www.natlawreview.com/article/california-s-delete-button-law-re-california-online-privacy-protection-act-caloppa.

162. CAL. BUS. & PROF. CODE § 22581(a)(3).

163. *Id.* § 22580(a), (i).

a Joint Statement of Principles with the Attorney General of California.[164] As part of this Statement of Principles, the operators voluntarily agreed to:

- "[P]rovide consumers with the opportunity to review the app's privacy policy *before downloading*";
- "[W]ork to educate app developers about their privacy obligations"; and
- "[D]evelop tools [for] consumers [to] report non-compliant apps."[165]

Given the creation of laws like CalOPPA and state laws prohibiting employers from requiring employees to provide their social media passwords, it is likely that states will continue to create laws to protect their citizens online.[166] It is also likely that there will be similar federal laws passed in regard to how websites, apps and Internet-connected devices operate, and to protect the data that they collect, especially when it comes to regulated industries like healthcare.[167]

B. *Health Data Laws and Regulations*

The care and feeding of privacy policies related to healthcare data are a special species, and as such, there are special laws that apply to its handling.[168] From the oath that physicians take that is the basis of their ethical obligations, to their patients and the practice of medicine, to laws intended to promote the adoption of electronic health records, there is quite a thicket of regulations that need to be considered when drafting a privacy policy for an app or website that captures and handles healthcare data.[169]

164. Troutman Sanders L.L.P., *Mobile App Developers and App Platforms Should Proactively Protect Users' Privacy*, INFORMATION INTERSECTION (June 3, 2013), http://www.informationintersection.com/2013/06/mobile-app-developers-and-app-platforms-should-proactively-protect-users-privacy/; *see also Joint Statement of Principles*, CAL. OFFICE OF THE ATTORNEY GEN. (Feb. 22, 2012).

165. Troutman Sanders L.L.P., *supra* note 164 (emphasis added).

166. *See* CAL. BUS. & PROF. CODE, §§ 22575–79; Troutman Sanders L.L.P., *supra* note 164.

167. *See* FOOD & DRUG ADMIN., *supra* note 67, at 7; Press Release, U.S. Dep't of Health & Human Servs., New Rule Protects Patient Privacy, Secures Health Information (Aug. 5, 2013), http://www.hhs.gov/news/press/2013pres/01/20130117b.html.

168. *See* Press Release, U.S. Dep't of Health & Human Servs., *supra* note 167.

169. *See id.*; *Hippocratic Oath*, NAT'L LIBR. MED. (Michael North trans.), http://www.nlm.nih.gov/hmd/greek/greek_oath.html (last updated Feb. 7, 2012).

1. The Hippocratic Oath

Healthcare privacy has its most basic roots in the Hippocratic Oath, an ancient Greek medical text which requires new physicians to swear that they will abide by certain professional ethical standards in their practice of medicine.[170] Though not required by most medical schools, the Hippocratic Oath has been adopted in various forms by some medical schools who have adapted it for modern times.[171] The Oath addresses the confidentiality of patient information, as physicians taking it state that "[w]hatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private."[172]

i. *The Hippocratic Oath in the Era of the Selfie*

Despite the Oath's lengthy history and emphasis on physicians making a serious commitment to the ethical standards of their profession, it seems that in the era of the *selfie*, the desire to try to become an Internet celebrity seems to be overcoming the commitment to ethical standards for some physicians.[173] Recent headlines have noted stories of surgeons texting or taking photos during procedures—in some cases resulting in allegations of malpractice and personal injury lawsuits.[174] Perhaps the most high profile such case is the wrongful death lawsuit filed by Melissa Rivers, the daughter of the late comedienne Joan Rivers, against the surgical center and physicians who operated on her mother.[175] The chief allegation in Rivers' lawsuit is that her mother's private physician, Dr. Gwen Korovin, not only performed an unauthorized biopsy procedure on Joan Rivers without the patient's consent but also took a selfie with the comedienne while she was under anesthesia.[176] In a statement, "Rivers' family lawyer Jeffrey Bloom said [that] doctors acted as *groupies*," with one doctor taking pictures of Korovin at work during the procedure and "that the [comedienne] 'would have been doing *Fashion Police* last week,' if [the doctors] had done their jobs."[177] The lawsuit goes on to allege that when Joan Rivers began to go

170. *Hippocratic Oath*, *supra* note 169.
171. *Id.*
172. *Id.*
173. *Id.*; *see also* Kory Grow, *Joan Rivers' Daughter Sues Medical Clinic over Comedian's Death*, ROLLING STONE (Jan. 27, 2015), http://www.rollingstone.com/tv/news/joan-rivers-daughter-sues-medical-clinic-over-comedians-death-20150127.
174. *See, e.g.*, Grow, *supra* note 173.
175. *Id.*
176. *Id.*
177. *Id.*

into cardiac arrest, the doctors did not perform a tracheotomy until seventeen minutes had elapsed, by which time Rivers had suffered irreversible brain damage.[178] It has been reported that the clinic may now "lose its federal accreditation in March," as an inquiry by Medicaid and Medicare investigators found errors that were made at the clinic, including "failing to note Rivers' weight before administering a sedative, allowing an unauthorized doctor in, and noting the cell phone photos" that were taken during the procedure.[179]

The age of paparazzi and reality television has intersected with the world of healthcare as part of the production of a number of healthcare television shows.[180] This interaction has brought to light new questions about healthcare privacy when a reality show is being filmed at a hospital.[181] In the case of the family of the late Mark Chanko, an eighty-three-year old investment advisor who was struck by a garbage truck and brought to New York Presbyterian Hospital, these questions have become all too real.[182] Unbeknownst to the family, the hospital was participating in the television show *NY Med*; and Chanko's treatment and ultimate death from his injuries had all been filmed; and the physician treating Chanko was wearing a hidden microphone.[183] His widow, Anita, did not realize this until she was watching the show one night and recognized her husband's voice calling for her on the show.[184] Even though his image had been blurred, and his voice changed to protect his identity, his wife recognized her husband's voice and was horrified to watch his treatment and death on television.[185] Adding to her horror was the fact that not only had she and her family not know that—according to their lawsuit—they were being filmed for the show, but also that they did not consent to said filming.[186] In 2013, the hospital was cited by the state for violating Mr. Chanko's rights, finding that "[t]he patient was unaware and uninformed that he was being filmed and viewed by a camera crew while receiving medical treatment thus his privacy in receiving medical treatment was not ensured."[187] The family has also sued the hospital, as well

178. *Id.*
179. Grow, *supra* note 173.
180. *See* Charles Ornstein, *Dying in the E.R., and on TV*, N.Y. TIMES, Jan. 4, 2015, at MB.1.
181. *See id.*
182. *Is Reality TV Compatible with the ER?*, HERE & NOW (Feb. 4, 2015), www.hereandnow.wbur.org/2015/02/04/reality-tv-compatible-er (audio file).
183. *Id.*
184. *Id.*
185. *See* Ornstein, *supra*, note 180; *Is Reality TV Compatible with the ER?*, *supra* note 182.
186. Ornstein, *supra* note 180.
187. *Id.*

as the physician.[188] While a state supreme court judge narrowed the lawsuit and allowed some of the family's claims to proceed, an appellate court dismissed the case, finding that "the doctor and hospital . . . did not breach their duty to avoid disclosing personal information since no . . . information was disclosed."[189] The family is now appealing and has reported the violation to the HHS Office for Civil Rights, which is investigating the report.[190]

The Chanko's called the hospital and spoke to one of its lawyers about who was responsible for the placement of the microphones to which the lawyer responded that ABC was responsible for placing the microphones on the physician treating Mr. Chanko.[191] According to Chanko's daughter-in-law, Barbara, who also happens to be a medical ethicist, the members of the television crew were all wearing scrubs, and—to the family—were not distinguishable from the nurses and physicians working on her father.[192] In an interview with National Public Radio ("NPR"), she questioned whether the hospital had a responsibility to inquire with its patient population as to whether it should allow such a show to film in the hospital.[193] Barbara Chanko also explained that the family has reported the incident to the Office for Civil Rights at the HHS, which investigates reports of HIPAA violations, though she noted that the HIPAA law concerns protecting information from being released to unauthorized parties, not patient privacy.[194]

She also questioned at what point is privacy violated in such a situation, is it if the camera crew is filming before the client gives consent?[195] Further, if the patient has been a victim of trauma, can he or she really understand the situation, let alone give informed consent?[196] Her inquiry continued, as she wondered how having a reality television show filmed in an emergency department impacts the patients and their treatment.[197] In this instance, the promotions for the episode of *NY Med* described the doctor who treated Chanko as *Dr. McDreamy-like*, and Barbara Chanko pointed out that the doctor treating her father-in-law seemed more interested in talking to the

188. *Id.*
189. *Id.*
190. *Id.*; *Is Reality TV Compatible with the ER?*, *supra* note 182.
191. *Is Reality TV Compatible with the ER?*, *supra* note 182.
192. *Id.*
193. *Id.*
194. *Id.*; *see also* Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104-191, § 1, 110 Stat. 1936, 1936.
195. *Is Reality TV Compatible with the ER?*, *supra* note 182.
196. *Id.*
197. *Id.*

camera during filming than treating his patient.[198] "The American College of Emergency Physicians opposes 'the filming for public viewing of emergency department patients or staff members except when they can give full informed consent prior to their participation' . . . ."[199]

The resulting debate among those in the medical community produced an ironic twist: Jeffrey Flier, the Dean of the Harvard Medical School, after reading about the Chanko case tweeted, "[h]ow could this be allowed to happen?"[200] Just four minutes later, the Chief of Surgery at Boston Medical Center, Dr. Gerard Doherty, replied via tweet that, "The same group is filming a trauma series at your place [Massachusetts General Hospital] and ours [Boston Medical Center] right now."[201] Unbeknownst to Flier, ABC News had been in Boston since October, filming at Massachusetts General and Brigham and Women's Hospitals for a documentary-style series called *Golden Hour* that would chronicle the care of patients in the hospitals' emergency rooms.[202] While he recalls watching similar shows and enjoying them, Flier said that after reading about the Chanko case, he is giving more thought to patient privacy and ethical concerns.[203] The Boston Globe reported that all three Boston hospitals signed contracts that "require consent from patients before their stories could be aired," and also "allow patients to change their minds and withdraw consent during filming, [as well as] within [thirty] days after the last filming of a patient."[204] The story also noted that this has already happened in at least three cases, and that the contract also allows the staff to ask the crew to stop filming at any time.[205]

ABC News has thus far defended itself in the Chanko case using a First Amendment defense, claiming that the show is protected because it is produced by the company's news division.[206] While it does not dispute that the crew did not obtain the family's consent, it also further moved that the claim should be dismissed because New York does not recognize a common law right to privacy, and that the Chanko family themselves were responsible

198. Ornstein, *supra* note 180; *Is Reality TV Compatible with the ER?*, *supra* note 182.

199. Ornstein, *supra* note 180.

200. Kay Lazar, *Patient Impact a Worry with TV Crews in ERs: Filming of Series in Boston Hospitals Stirs Debate on Balancing Privacy Concerns, Public Benefit*, BOSTON GLOBE, Jan. 12, 2015, at B1.

201. *Id.*

202. *Id.*

203. *Id.*

204. *Id.*

205. Lazar, *supra* note 200.

206. Ornstein, *supra* note 180.

for their loss of privacy.[207] ABC News has released a statement about the case:

> We are very sorry about Mark Chanko's tragic and untimely death. We sympathize with his family over their loss. We worked hard in our N.Y. Med broadcast to obscure his image and identity and the identity of his family.
>
> We are very proud of our acclaimed series of medical programs showing up close the work and humanity of doctors, nurses, residents and other health care professionals at the top medical academic centers in the country, including Johns Hopkins, New York Presbyterian, Mass General, Brigham and Women's, Boston Children's Hospital, Boston Medical Center and other great medical institutions.
>
> We strive always to be highly respectful of the patients, their families and the hospital caregivers. We have heard many stories of people inspired after seeing our programs to pursue medical professions, to seek treatment they wouldn't have known about or been too frightened to pursue or to become organ donors after seeing depictions of successful transplants.[208]

The Chanko case is hardly the first lawsuit resulting from the filming of a reality show in a hospital and will probably not be the last as devices capable of recording patient identity and date creep into more and more aspects of our lives.[209] In the early 2000s, the New York Times Co. was sued for invasion of privacy by a group of patients who were featured in the show *Trauma: Life in the E.R.*[210] Many of the plaintiffs settled, but in one case an appeals court ruled in favor of the production company, finding that the show qualified as news, and was protected under the law.[211] The intersection of reality television, the IoT, and healthcare will be likely to produce more interesting questions as to what is news and what is an invasion of privacy in coming years; it will be interesting to see what results.

It remains to be seen how the case law will develop in regard to the filming of patients in medical facilities during treatment, particularly in the age of smartphones and the IoT. Where there are failures on the part of health care professionals to respect their duty to keep patient information and data confidential, the task of regulating and disciplining them falls to state

207. *Id.*
208. *Is Reality TV Compatible with the ER?*, *supra* note 182.
209. *See* Ornstein, *supra* note 180.
210. *Id.*
211. *Id.*

professional licensing boards, as well as hospital credentialing committees.[212] These bodies are often the epicenter of disciplinary trends in health care, and they will be a crucial part of the adoption and regulation of IoT devices.[213] It will be important that these entities stay on top of developments in terms of new applications and devices, and their impact on patient data, so that they can draft and implement policies to appropriately address them.[214]

In the case of hospitals, data and public image are more important than ever. The implementation of section 3025 of the Affordable Care Act ("ACA") added section 1886(q) to the Social Security Act, which established the Hospital Readmissions Reduction Program.[215] The establishment of this program brought with it a new reality: That hospitals would lose Medicare reimbursement dollars in instances where patients over the age of sixty-five are readmitted to the hospital for heart failure, pneumonia, or acute myocardial infarction.[216] Section 3008 of the ACA also resulted in the creation of the Hospital-Acquired Condition ("HAC") Reduction Program, which aims to reduce the occurrence of preventable conditions that patients did not have upon admission to a hospital, but developed during a hospital stay.[217] In addition, the data about these readmission and infection rates has been made available to the public as never before, and thus giving consumers the ability to shop between hospitals based on their patient data for conditions like pneumonia and urinary tract infections.[218] This increased pressure on hospitals to improve readmission rates and reduce hospital acquired infections will likely result in these facilities keeping a keen eye on the implementation of new, Internet connected devices and how they impact patient outcomes, as well as hospitals' public images.[219] As hospitals collect more and more patient data, the protection of that data will be paramount to not only complying with the related healthcare privacy laws, but also maintaining consumer trust in their ability to do so.

212. 42 U.S.C. § 1320a–7e (2012); Koenig, *supra* note 36, at 17.

213. *See* INTEL, *supra* note 102, at 3.

214. *See id.*

215. *See* 42 U.S.C. § 1395ww(q)(1).

216. *See id.*; *Hospital-Acquired Condition (HAC) Reduction Program*, CENTERS FOR MEDICARE & MEDICAID SERVICES, http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/AcuteInpatientPPS/HAC-Reduction-Program.html (last modified Dec. 18, 2014); INTEL, *supra* note 102, at 1.

217. 42 U.S.C. § 1395ww(p)(1); *see also Hospital-Acquired Condition (HAC) Reduction Program*, *supra* note 216.

218. *See Hospital-Acquired Condition (HAC) Reduction Program*, *supra* note 216.

219. *See id.;* INTEL, *supra* note 102, at 4.

2. Confidentiality of Alcohol and Drug Abuse Patient Records

Another aspect of the web of medical privacy laws can be found at 42 C.F.R. § 2, which sets out privacy provisions for the records of the identity, diagnosis, prognosis, or treatment of patients that are maintained as part of a federally assisted drug or alcohol abuse program.[220]

3. Medicare Conditions of Participation

A significant requirement in terms of privacy for most healthcare providers and facilities comes in the form of the Medicare Conditions of Participation, codified 42 C.F.R §§ 482 to 486.[221] The Conditions for Participation for hospitals, home health agencies, states, long-term care facilities, and suppliers all require these entities to safeguard patient records from disclosure, and not to release them without the patient's consent.[222]

4. HIPAA

The most prominent privacy law when it comes to healthcare is HIPAA.[223] Passed in 1996, this law protects the privacy of individually identifiable health information, which it defines as information that

> relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[224]

HIPAA applies only to certain entities, which it refers to as *covered entities*, and includes "health plan[s], . . . healthcare clearinghouse[s], [and] a healthcare provider who transmits any health information in electronic form."[225] It is the latter category where it is likely that change will be needed as the IoT devices, particularly those related to healthcare mature, and regulatory solutions to protect healthcare data become apparent.[226] As it currently stands, HIPAA does provide covered entities with an exemption

220. 42 C.F.R. § 2 (2014).
221. *Id.* §§ 482.1–486.348.
222. *Id.* § 2.3; *see also* 42. C.F.R. §§ 482.1–486.348.
223. Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104-191, § 1, 110 Stat. 1936.
224. *Id.* § 1320d(B).
225. 45 C.F.R. § 160.103 (2013) (*Covered entity*).
226. *See* INTEL, *supra* note 102, at 3–4.

that allows them to use or disclose protected health information in order to provide treatment, obtain payment, or carry out other healthcare operations as set forth in the statute.[227]

5. HITECH Act

A major factor in the growth of healthcare data and related issues is the implementation of the HITECH Act of 2009.[228] This law was intended to provide a monetary incentive for hospitals and healthcare providers to convert to electronic medical records systems, and it covers medical records and patient information in oral, paper, or electronic form.[229] The passage of the HITECH Act also made significant changes to both the enforcement and sanctions as they relate to the healthcare privacy and security requirements enacted as part of HIPAA.[230] One of these changes was the shift of the enforcement authority of the provisions of HITECH to the HHS from the Office for Civil Rights and the Centers for Medicare and Medicaid Services ("CMS").[231] While some agencies retain certain interests in the enforcement of HITECH, the primary enforcement after the implementation of the law lies with HHS.[232] In addition, state attorney generals can bring an action in federal court on behalf of their respective state residents.[233]

The HITECH Act places privacy obligations on not only covered entities, but also on the business associates who provide services to those covered entities, and may handle personal health information.[234] This means that these business associates are subject to the same physical, technical, and administrative security requirements as those that covered entities must follow under HIPAA.[235] These business associates can include lawyers, IT personnel, benefits consultants, and accountants.[236] Typically, the compliance requirements imposed upon business associates are addressed in the terms of a business associate contract.[237] Under the Omnibus Rule that

227. 45 C.F.R. § 164.506(a), (c).

228. 42 U.S.C. § 300jj (2012).

229. Health Information Technology for Economic & Clinical Health Act of 2009, Pub. L. No. 111-5, § 13001, 123 Stat. 115, 175 (2009); *see also* 45 C.F.R. §§ 160.103 (*Covered entity* and *Health Information*), 160.402(a), 162.923(a), 164.103 (*Required by law*).

230. Health Information Technology for Economic & Clinical Health Act §§ 13401, 13410; *see also* 45 C.F.R. §§ 160.402(a)–(c), .404(a)–(b), 164.306(a)–(e).

231. 42 U.S.C. § 17939.

232. *See id.*

233. 42 U.S.C. §1320d-5(d)(1) (2012).

234. Health Information Technology for Economic & Clinical Health Act § 13401; *see also* 45 C.F.R. § 160.103 (*Business associate*) (3)(i)–(iii).

235. *See* 45 C.F.R. § 160.103 (3)(i)–(iii).

236. *See id.*; 160.103 (*Business associate*) (i)–(ii).

237. 42 U.S.C. §17938 (2012).

made modifications to the HIPAA and HITECH laws, business associates are now directly subject to some of the requirements of the HIPAA Privacy Rule, including providing a notice of privacy practices or designating a privacy officer in the event that the business associate delegates that obligation to a third party.[238] In addition, the Omnibus Rule allows business associates of covered entities to disclose protected health information to a business associate who is a subcontractor.[239] As part of this change, the business associate can allow the subcontractor to create or receive that PHI on its behalf, so long as the business associate obtains adequate assurances from the subcontractor that it will safeguard the information.[240] This change passes the responsibility of obtaining such assurances from being that of the covered entity to being the responsibility of the business associate, but is still done through a business associate agreement, which lays out the responsibilities and obligations of the respective parties.[241]

Other important aspects of the HITECH Act are the requirements that it imposes upon covered entities and business associates in terms of security breach notifications.[242] The Act defines a breach as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not . . . have been able to retain such information."[243] The Act further defines unsecured personal health information as information that is not protected "through the use of a technology or methodology specified by the Secretary in . . . guidance . . . that renders the [PHI] unusable, unreadable, or indecipherable to unauthorized individuals."[244]

6. ACA

Yet another significant law when it comes to healthcare privacy is ACA.[245] This law created the Health Insurance Marketplace, as well as the website HealthCare.gov, where consumers can shop for insurance policies

238. *See id.*; 45 C.F.R. §§ 164.308(b), .502(e)(2).
239. *See* 42 U.S.C. §17938; 45 C.F.R. § 160.103(3)(iii).
240. 42 U.S.C. § 17938; 45 C.F.R. § 160.103(3)(iii).
241. *See* 42 U.S.C. §17938; 45 C.F.R. § 160.103(3)(iii).
242. *See* 42 U.S.C. § 17921(1)(A), (2).
243. *Id.* § 17921(1)(A).
244. 42 U.S.C. § 17932(h)(1)(a)–(b).
245. *See* Patient Protection & Care Affordable Act of 2010, 42 U.S.C. § 18001 (2012); *see also* Anna North, Op-Ed, *Is Your Obamacare Data Safe?*, N.Y. TIMES, Jan. 25, 2015 (Late Edition), at SR. 10.

available through the federal marketplace.[246] The law also requires insurance companies to cover people with pre-existing health conditions, allows coverage to continue for young adults up to age twenty-six under their parents' policies, and makes it illegal for health insurance companies to cancel coverage just because an insured person gets sick.[247]

As with many new healthcare laws, the implementation of ACA has not been without bumps in the road.[248] In addition to challenges by politicians who are not fans of the new law, there have been privacy concerns that have emerged as the HealthCare.gov website has rolled out.[249] This website serves as the hub for consumers to sign up for health insurance, as well as the marketplace for them to shop for policies.[250] As one can imagine, this process involves a lot of sensitive data, which consumers and regulators are very concerned about keeping safe.[251] However, as recent headlines have detailed, an Associated Press report said that the site has been sharing user data, including users' ages, income levels, and whether they are pregnant or not, with third parties like Facebook, Twitter, and Google.[252] These reports highlighted new privacy concerns that have arisen as the IoT expands: First, that of broken promises of anonymization; and second, "'the spillage of data from one context into others.'"[253] The concerns in the first instance focus on situations where the organization collecting the data assured users that the data would be made anonymous, but it is then either not made anonymous, or the process is not carried out well.[254] The second concern relates to situations where health data is collected in one context, but then used by a third party in ways that consumers are not aware of and may not have necessarily consented to under the terms of the first context.[255]

Officials from CMS have emphasized that they do not and will not sell visitor information from HealthCare.gov, and that they remain vigilant about working to make sure that consumer data is protected.[256] Aaron Albright, director of the media relations group at CMS, explained that

246. *Rights & Protections*, HEALTHCARE.GOV, http://www.healthcare.gov/health-care-law-protections/.
247. *Id.*
248. *See* North, *supra* note 245.
249. *Id.*
250. *Rights & Protections*, *supra* note 246.
251. *See* North, *supra* note 245.
252. *Id.*
253. *Id.*
254. *Id.*
255. *Id.*
256. North, *supra* note 245.

> "Private sector tools . . . play a critical role in the operation of a consumer focused website. Without these tools, HealthCare.gov would be unable to effectively respond to system errors, issues that result in a poor or slow web experience, or provide metrics to the public on site visits [or] mobile usage. In addition, consumers would have to continuously resubmit information throughout the process making signing up for insurance more difficult."[257]

This explanation highlights the tension between consumer demands for user-friendly websites, as well as for sites that protect consumer data to the greatest extent possible.[258] As with many types of software projects, this tension must be weighed against the business decision that often must be made between using a third party tool or taking the extra time and money to build such a tool internally.[259]

7. Genetic Information Nondiscrimination Act of 2008 ("GINA")

An important privacy law that has been enacted to protect patient health information is GINA.[260] This law states that *genetic information* is PHI, and is protected under HIPAA.[261] It further prohibits health insurance companies from using genetic information for underwriting purposes and prohibits employers from discriminating against people based on such information.[262]

The passage of the GINA law, as well as the updates to it as the HIPAA and HITECH laws have evolved, represent an important line of defense to protect patients against discrimination on the basis of genetic information.[263] This defense will only continue to grow in importance as personalized medicine based on genetic information is used more widely and as more is discovered about the impact of genetics on human health.[264] It is also likely that as other categories of health data are discovered that laws will

257. *Id.*
258. *Id.*
259. *See id.*
260. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2008); Press Release, U.S. Dep't of Health & Human Servs., *supra* note 167.
261. Genetic Information Nondiscrimination Act § 1180(a)(1); Press Release, U.S. Dep't of Health & Human Servs., *supra* note 167.
262. Genetic Information Nondiscrimination Act § 1180(a)(2); Press Release, U.S. Dep't of Health & Human Servs., *supra* note 167.
263. Genetic Information Nondiscrimination Act § 1180(a); Press Release, U.S. Dep't of Health & Human Servs., *supra* note 167.
264. Press Release, U.S. Dep't of Health & Human Servs., *supra* note 167.

be passed to protect against discrimination based on what can be gleaned from that data.[265]

C. *Impact of Internet of Things on Health Laws*

1. Hesitancy of Healthcare Providers

Despite the great potential of the use of big data in healthcare, there is also evidence of hesitancy on the part of providers to implement some tools until they are fully baked.[266] A recent NPR story noted how a doctor at Stanford's Lucile Packard Children's Hospital searched patient record data to examine treatment of pediatric lupus patients, and eventually find a way to save the life of such a patient, but that ultimately the hospital opted not to continue doing so, as the doctors felt that the system for mining such patient data was not yet ready for prime time.[267] While it is noted in the story that the ability to search such data can fill the gap in situations where there is not sufficient published literature to help doctors navigate difficult cases, there does seem to be a consensus among some hospitals and physicians that these systems need to be better developed before they are widely adopted.[268] This applies not only to systems to mine patient data to find solutions, but also to electronic medical records systems.[269] In some instances, hospitals have begun to mine the data present in their records, but found that they are not yet ready to do this in all of their cases, as was discovered by Dr. Jenny Frankovich, an attending physician at the Stanford Lucile Packard Children's Hospital.[270] As Dr. Frankovich explained in her NPR interview, while her analysis of the treatment of other pediatric lupus patients from the data from their respective charts in the database helped her find a solution to treat her patient in that instance, the physicians have not yet instituted this practice on a widespread basis, as they feel that the system is not yet ready in terms of accuracy and reliability to be used in every case.[271]

265. *See id.*

266. *See, e.g.*, *Big Data Not a Cure-All in Medicine*, NPR (Jan. 5, 2015, 4:22 PM), http://www.npr.org/2015/01/05/375201444/big-data-not-a-cure-all-in-medicine.

267. *Id.*

268. *See id.*

269. *Id.*

270. *Id.*

271. *Big Data Not a Cure-All in Medicine*, *supra* note 266.

2. Imposition of Health Privacy Laws on New Categories of People

i. *Web Developers, App Developers, Tech Companies*

An interesting aspect of the issues that develop at the intersection of the growth of the Internet of Things and healthcare are those faced by the parties that support the entities that are bound by HIPAA and other medical data protection laws, including web developers.[272] Development of healthcare websites has grown exponentially, especially given the fact that, according to a 2013 study by the Pew Internet and American Life Project, "[o]ne in three American adults have gone online [to try] to figure out [what] medical condition" that they or another individual might have.[273] Of those individuals who searched for a medical condition online, forty-six percent said that the information led them to think that they needed the attention of a medical professional, and thirty-eight percent said that they used it to determine if the condition was something that they could take care of at home, and eleven percent said it was both reasons or somewhere in between.[274] The increased use of online medical information has made the online presence of medical device manufacturers, pharmaceutical companies, physicians, hospitals, and other related entities have a presence on the web.[275] As such, they are increasingly reaching out to web and app developers to help them create such a presence, and in instances where such developers have to interact with patient data, to ensure HIPAA compliance.[276]

The changes to the HIPAA and HITECH laws as a result of the implementation of the Omnibus Rule have made taking on the obligations of abiding by these healthcare data privacy laws a bit clearer for developers, as it better lays out the obligations of business associates handling PHI, as well as the circumstances under which a developer could opt to use a subcontractor who is more familiar with the obligations and procedures for handling sensitive data rather than taking on all of the obligations themselves.[277] The developers remain responsible for oversight in such a situation, but they also can make sure that both parties are clear as to their roles through the use of a well-drafted business associate agreement.[278]

272. Wang, *supra* note 21.

273. Susannah Fox & Maeve Duggan, *Health Online 2013*, PEWRESEARCHCENTER (Jan. 15, 2013), www.pewinternet.org/2013/01/15/health-online-2013/.

274. *Id.*

275. *Id.*

276. *See id.*; Wang, *supra* note 21.

277. *See* 45 C.F.R. § 160.103(3)(iii); Press Release, U.S. Dep't of Health & Human Servs., *supra* note 167.

278. *See* 45 C.F.R. § 502(c), (d).

Further, as healthcare companies have become more experienced in dealing with developers, they are in some instances becoming more adept at training them as to how to comply with relevant data privacy laws.[279] In other words, regulatory agencies seem to be picking up the slack, and will likely get the message across through enforcement actions for those who do not ensure their apps and devices comply, as the FTC has done with recent COPPA actions.[280]

3. FDA Regulation of Health Apps and Devices

At the time of this writing, there were more than 43,000 healthcare apps available in the Apple iTunes App Store.[281] However, of these apps, an October 2013 survey by the IMS Institute for Healthcare Informatics found that most of these apps had only been downloaded fewer than 500 times, and very few offered any type of robust functionality.[282] In the worst cases, the apps provided *inaccurate or unproven* information, some even in apps designed for clinical use by physicians![283] This new reality of healthcare apps has caught the attention of the FDA, as it seeks to protect people from inaccurate or unsafe information that may be provided in healthcare apps or devices.[284] In September of 2013, the FDA announced that it would start regulating healthcare apps, focusing on those apps that "meet the regulatory definition of *device*, and that (i) are intended to be used as an accessory to a regulated medical device, or (ii) transform a mobile platform into a regulated medical device."[285] The FDA noted that the agency has extensive resources available to help app developers determine the level of regulation that applies to their particular product, such as the *Product Classification Database* and the *510(k) Premarket Notification Database*, and to stay up-to-date on new information about changes to these regulations.[286]

The FDA has provided examples of specific apps that have been approved under its new regulations, as well as examples of the types of apps and devices that would be subject to these regulations.[287] The first category of apps the FDA will be regulating are "[m]obile apps that transform a

279. *See id.*
280. *See* Fair, *supra* note 152.
281. Litt, *supra* note 16.
282. *Id.*
283. *Id.*
284. FOOD & DRUG ADMIN., *supra* note 67, at 4; Litt, *supra* note 16.
285. *Mobile Medical Applications*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm255978.htm (last updated June 4, 2014).
286. *Examples of MMAs the FDA Regulates*, *supra* note 107.
287. FOOD & DRUG ADMIN., *supra* note 67, at 13−15, 20–22.

mobile platform into a regulated medical device and therefore are mobile medical apps."[288] The FDA's guidance states that this category would include apps that use sensors attached to the mobile platform or tools within the mobile platform to diagnose a condition, as well as those that "present donor history questions to a potential blood donor and . . . transmit the [answers to] . . . a blood collection facility" to determine the donor's eligibility to donate blood.[289] The second category of apps that the FDA will now regulate are those "apps that connect to an existing device type for purposes of controlling its operation, function or energy source, and therefore are mobile medical apps."[290] The guidance states that this category would include apps that control or monitor devices such as infusion pumps, neuromuscular stimulators, or blood pressure cuffs.[291] The third category of apps that are now covered by FDA regulation are "mobile apps that display, transfer, store, or convert patient-specific medical device data from a connected device and therefore are mobile medical apps."[292] Included in the examples for this category are

> apps that connect to a nursing central station and display medical device data to a physician's mobile platform for review, . . . apps that connect to bedside—or cardiac—monitors [that] transfer the data to a . . . viewing station for . . . patient monitoring, . . . [as well as] apps that connect to a perinatal monitoring system and transfer . . . contraction and fetal heart rate . . . to another display to allow for . . . monitoring [the] progress [of a patient's labor].[293]

The announcement of these new regulations for healthcare apps caused plenty of grumbling in fast-paced Silicon Valley, where the focus is often on being the first to market, and there is typically lower tolerance for lengthy regulatory processes.[294] However, the FDA has made it clear that going forward, device and app developers looking to create IoT products and services for the healthcare industry will need to play by their rules in order to operate in this space.[295] There will likely be some growing pains, but one hopes that as developers learn the ropes of the FDA procedures, and take advantage of the huge potential market for smart healthcare devices and

288. *Examples of MMAs the FDA Regulates*, *supra* note 107.
289. *Id.*
290. *Id.*
291. *Id.*
292. *Id.*
293. *Examples of MMAs the FDA Regulates*, *supra* note 107.
294. *See* FOOD & DRUG ADMIN., *supra* note 67, at 4.
295. *See id.*

apps, that the process of complying with the regulations will become less painful.

4. Conflicts in Terms of Service and Privacy Policy

Among the legal challenges presented by the growth of the IoT as it relates to healthcare is how developers can not only write privacy policies for their devices or services that comply with applicable privacy laws, but also ensure that they work with the policies of other products in that ecosystem.[296] As the universe of apps has exploded in recent years, conflicts between the terms of use and privacy policies of different apps and platforms have become more common.[297] Such conflicts became apparent to this author when she installed an app on her tablet called SnapHack, which allows users to save their SnapChat messages, which typically only last between one to ten seconds.[298] The SnapHack app interfaces with SnapChat through its applied programming interface, or API, and more interestingly, the app features a disclaimer in its terms of service that states that the developers of SnapHack are not responsible if the use of its app violates the terms of use for SnapChat and results in the user's SnapChat account being deleted.[299] As the IoT ecosystem matures, it will be important for developers to work to ensure that their apps do not violate the terms of use for another app or platform in such a way that might result in users' accounts being deleted. While it may be upsetting in the short term for a user to lose his or her SnapChat messages, one can imagine how devastated a user of a healthcare app would be to lose months or years of health data that he or she has been using to track a serious medical condition.

As well as conflicts between the terms of use and privacy policies of apps, there are also real world legal consequences of developers creating apps using pieces of software that are not in compliance with privacy laws.[300] The FTC recently took the unprecedented step of warning app developer

296. *See* FED. TRADE COMMISSION, *supra* note 5, at viii.

297. *See, e.g.*, *id.* at vii−viii.

298. *See* Salvador Rodriguez, *SnapHack App Lets Users Save Snapchat Photos Without Notifying Sender*, L.A. TIMES (Oct. 14, 2013, 1:19 PM), http://www.latimes.com/business/technology/la-fi-tn-snapchat-snaphack-save-photos-20131014-story.html.

299. Charlie Osborne, *Snapchat Issues Outright Ban on Third-Party Apps Following 4chan Hack*, ZDNET (Nov. 17, 2014, 12:30 GMT), http://www.zdnet.com/article/snapchat-issues-outright-ban-on-third-party-apps-following-4chan-hack/.

300. *See* 16 C.F.R. § 312.3 (2012); Press Release, Fed. Trade Comm'n, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations, (Dec. 22, 2014) http://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa.

BabyBus that its apps were not in compliance with COPPA, and that it could face fines if it did not take steps to bring them into compliance.[301] It turned out that the problem was not with BabyBus' software code in the app, but with a third party API that was collecting data subject to COPPA from minors and did not have the applicable compliance and parental consent mechanisms in place.[302] As a result of the warning, Google pulled all of the BabyBus apps from the PlayStore until they were in compliance with the law.[303] Situations like this illustrate the importance for developers to not only work to ensure that they have policies and procedures in place so that their products are in compliance with applicable privacy laws, but also do their due diligence in terms of third party software to make sure it does as well.[304] Given the growing thicket of regulations and laws governing the protection of healthcare data, taking these steps will be more important than ever for developers in the IoT healthcare space.[305] As much as the FTC is stepping up its COPPA enforcement actions, it is likely that the Commission, as well as the FDA, will do the same as it relates to apps and devices in the IoT in healthcare, and not being in compliance could result in expensive lessons in terms of fines, as well as negative publicity.[306]

5. Interoperability issues

In addition to the myriad legal considerations that come with the era of the IoT for healthcare, there are also an equal number of practical considerations that must be addressed as part of the implementation process.[307] One such consideration is the interoperability of all of these devices and applications.[308] As mentioned above, there is hesitancy among some physicians and hospitals in the midst of the implementation of so much technology at this time, and interoperability is a big part of that concern.[309] Developers and manufacturers of IoT devices and apps will have to tread

301. *See* 16 C.F.R. § 312.3; Press Release, Fed. Trade Comm'n, *supra* note 300.

302. 16 C.F.R. § 312.3; Wendy Davis, *Google Suspends BabyBus Apps After FTC Warns of Privacy Violations*, MEDIAPOST (Dec. 29, 2014, 4:50 PM), http://www.mediapost.com/publications/article/240860/google-suspends-babybus-apps-after-ftc-warns-of-pr.html; Press Release, Fed. Trade Comm'n, *supra* note 300.

303. Davis, *supra* note 302.

304. *See id.*; Press Release, Fed. Trade Comm'n, *supra* note 300.

305. *See* Davis, *supra* note 302; Press Release, Fed. Trade Comm'n, *supra* note 300.

306. *See* Press Release, Fed. Trade Comm'n, *supra* note 300.

307. *See* INTEL, *supra* note 102, at 1.

308. *Id.* at 3.

309. *See id.* at 3; *supra* Part III.C.1.

carefully, and involve doctors and hospitals in the development of their products to make sure these products can become part of the IoT ecosystem and work with other products in it if they want to succeed.[310] As Dr. Michael Blum, a cardiologist at the University of California, San Francisco, noted on a recent NPR story, doctors are getting pitches from entrepreneurs on a near daily basis, and while "[t]heir perspective is, '[y]ou old doctors have kept things the same as they are for [fifty] years. [We have] got [sic] new technology, and [it is] going to disrupt healthcare' . . . . [But] [t]he [p]roblem is just because a device looks shiny and new [does not] mean [it is] useful."[311] Blum said that in many instances, validation studies are needed, and the task of carrying out these studies often falls to doctors and hospitals, so developers will also need to allow time in their product planning.[312] The implementation of the new FDA guidelines for medical devices and apps should help with this process, whether developers like it or not.[313]

6. BYOD

A practical reality related to interoperability is bring your own device ("BYOD") to hospitals and healthcare facilities.[314] Where in the past corporations had certain standard devices that all employees used, the proliferation of smart phones and devices in society now means that physicians and nurses all have a variety of personal and professional devices, and that any platform a hospital or healthcare system adopts must work with a broad spectrum of devices.[315] The same goes for patients, so developers must consider what platforms patients are using, and make sure that their products work well with those platforms to help with their widespread adoption.[316]

This BYOD reality makes the concerns about interoperability, both in terms of policies and operation, even more important for new IoT devices and applications.[317] The challenge will be how to find products that allow medical professionals easy and fast access to patient data detected by IoT devices, while also building in security measures to protect that same data.

---

310. *See* Sullivan, *supra* note 17.
311. Standen, *supra* note 16.
312. *Id.*
313. INTEL, *supra* note 102, at 3–4.
314. *BYOD*, HEALTHCARE IT NEWS, http://www.healthcareitnews.com/directory/byod (last visited Aug. 22, 2015).
315. *See id.*
316. *See id.*
317. *See id.*

7. Recalls

Ultimately, given the legal and practical considerations of the IoT as it relates to healthcare, there will need to be solutions on both fronts to protect healthcare data.[318] One such solution is that of recalls of medical devices.[319] To date, there have not been any such recalls for cybersecurity reasons, but it is foreseeable that this could change in the future with the explosion of medical devices that are part of the IoT.[320] The challenges could be said to be twofold: First, those presented by the rise of three-dimensional printing, and, second, the related—but in many instances separate—challenges presented by the rise of crowdfunding as a means of funding medical device challenges.[321] In the first instance, while three-dimensional printing has allowed physicians to print prostheses to create lifesaving solutions for patients, these prostheses were not subject to the same rigors that traditional solutions undergo as part of research and development, and their long-term consequences remain to be seen.[322] However, the same can be said of devices that go the traditional development route.[323] In the instance of some metal hip replacements, this oversight did not prevent problems with the implants that caused devastating injuries to patients when they began to lock up and shed metal shavings into their bloodstreams.[324]

The challenge that both three-dimensional printing and crowdfunding present is that in some instances, unlike traditional pharmaceutical and medical device manufacturers, these products are starting to be developed by small or independent companies that may not have the same corporate legacy in terms of incorporation and continued corporate existence.[325] This legacy is important, as in the case of device recalls, government agencies, as well as consumers, would need to be able to contact the company and its customers to inform them of said recall.[326] Though this

318. *See supra* Part II.

319. *See* Poremba, *supra* note 62.

320. *Id.*

321. *See* Lucy Vernasco, *3-D Printing Is Changing the Future of Prosthetics*, DAILY BEAST (Dec. 10, 2014, 5:45 AM), http://www.thedailybeast.com/articles/2014/12/10/3-d-printing-is-changing-the-future-of-prosthetics.html; Alex Wawro, *Washington Sues Kickstarted Game Creator Who Failed to Deliver*, GAMASUTRA (May 2, 2014), http://www.gamasutra.com/view/news/216887/Washington_sues_Kickstarted_game_creator_who_failed_to_deliver.php.

322. *See* Vernasco, *supra* note 321.

323. *See* Barry Meier, *Maker Aware of 40% Failure in Hip Implant*, N.Y. TIMES, Jan. 22, 2013, at A1.

324. *Id.*

325. *See* Vernasco, *supra* note 321; Wawro, *supra* note 321.

326. Meier, *supra* note 323; *see also* Poremba, *supra* note 62.

concern is less likely for the companies creating devices and apps subject to the FDA regulations, there is still a concern for those companies or inventors that are not covered by them.[327]

As the IoT for healthcare develops, the Agency may have to help fill the gap between established companies and startups, or other parties may have to step up.[328] This has already started to happen on the crowdfunding front, as popular crowdfunding sites like Kickstarter and game platform Steam Early Access changed their terms of service in September to require that creators actually deliver the products and rewards described in their campaign.[329] This move was motivated by the backlash from backers in response to several game campaigns that never delivered as promised, or else delivered low quality games.[330] State attorneys general are monitoring the crowdfunding space from a consumer protection law standpoint as well, as the Attorney General for the State of Washington filed what is believed to be the first consumer protection lawsuit concerning crowdfunding against Kickstarter game creator Edward J. Polchlepek III—also known as Ed Nash—and his company Altius Management, in May of 2014.[331]

IV. CONCLUSION

Much as it did in the time of Justices Brandeis and Warren in the age of snapshot photography, concerns about privacy remain just as paramount among consumers and regulators today in the age of the IoT.[332] Given the importance of keeping consumers and their data safe in this fast-paced age of rapid technological development, it will be crucial for regulators to keep an eye on how these technologies are developing, as well as collect and analyze data, so that they can develop solutions to the problems that may crop up along the way. Lawyers will also play an important role in this process, as they defend victims of data breaches and hold retailers and data aggregators accountable for the protection of consumer data. Lawyers will also play an

327. *See* FOOD & DRUG ADMIN., *supra* note 67, at 13–18; Standen, *supra* note 16; Sullivan, *supra* note 17.

328. *See* INTEL, *supra* note 102, at 2–4; Poremba *supra* note 62; Sullivan, *supra* note 17.

329. Jeff Grubb, *Valve Expands Its Rules for Early Access Games on Steam*, VENTUREBEAT (Nov. 20, 2014, 11:45 AM), http://venturebeat.com/2014/11/20/valve-expands-its-rules-for-early-access-games-on-steam/; Christian Nutt, *Kickstarter Updates Terms: 'The Creator Must Complete the Project'*, GAMASUTRA (Sept. 19, 2014), http://www.gamasutra.com/view/news/226071/Kickstarter_updates_terms_The_creator_must_complete_the_project.php.

330. Wawro, *supra* note 321; *see also* Nutt, *supra* note 329.

331. Wawro, *supra* note 321.

332. *See* Warren & Brandeis, *supra* note 1, at 195; Greenough, *supra* note 6.

integral role in the care and feeding of privacy policies as they relate to the IoT and healthcare, as well as other industries, advising companies as to how best to develop their policies and procedures, as well as how to communicate them to patients and regulators.

There is perhaps no other industry that this process will be more important than in healthcare. As such, the solutions developed by entities, from hospitals to state and federal healthcare agencies to app developers, will shape the role of the IoT in the future of healthcare.