THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XX STLR.ORG SPRING 2019

ARTICLE

THE CHATBOT WILL SEE YOU NOW: PROTECTING MENTAL HEALTH CONFIDENTIALITY IN SOFTWARE APPLICATIONS†

Scott Stiefel*

Chatbots are a form of artificial intelligence that can read text, or translate voice to text, and provide a response. While they have existed since the 1960's, they have recently been used to provide a form of therapy through software applications ("apps"). However, unlike licensed professionals who provide traditional mental health services, chatbots are not subject to confidentiality obligations. Currently, federal and state regulations that impose confidentiality obligations in the healthcare context do not apply to chatbots, and the regulations that do apply to chatbots do not impose such obligations. Because users engaging with these apps disclose information similar to information disclosed during a therapy session, this Article proposes a new regulatory framework, through new legislation, to limit the use and disclosure of information received by software-based therapy technologies.

* Corporate Counsel - Henry Schein One, Internet Brands. LL.M. in Health Law, Loyola University Chicago; J.D., The Catholic University of America; B.S., University of Illinois at Urbana. For her patience, guidance, and assistance, I am grateful to Nadia Sawicki, my thesis advisor. I am also thankful for the assistance and input of Stacey Tovino, Jordan Paradise, and the editorial team at the Columbia Science & Technology Law Review.

I. INTRODUCTION

Instead of a therapist, the chatbot will see you now.[1] Chatbots, a form of artificial intelligence, can read text, or translate voice to text,

1. *See, e.g.*, Megan Molteni, *The Chatbot Therapist Will See You Now*, WIRED (June 7, 2017), https://www.wired.com/2017/06/facebook-messenger-woebot-chatbot-therapist (discussing the creation of Woebot); Nick Romeo, *The Chatbot Will See You Now*, NEW YORKER (Dec. 25, 2016), https://www.newyorker.com/tech/annals-of-technology/the-chatbot-will-see-you-now (discussing the creation of X2AI, a chatbot therapist).

and provide a response.[2] While chatbots have existed since the 1960s,[3] they have only recently been used to provide a form of therapy through a software application ("app").[4]

Therapy, counseling, and other mental health treatment and assistance have traditionally employed a therapist, psychologist, or other mental health professional to talk with an individual.[5] Professionals practicing in these areas are subject to various licensing restrictions and requirements, which vary by state.[6] Paramount to these professionals' obligations is the responsibility to maintain patient confidentiality and, in some cases, to maintain information subject to the patient-therapist privilege.[7]

Chatbots, however, are not subject to these professional obligations. In lieu of state licensure requirements, chatbots operating in the mental health space may be subject to oversight by the Food and Drug Administration ("FDA") as medical devices.[8] Chatbot creators argue that their apps do not provide "treatment," but provide "support" or "chat," likely in an effort to evade oversight from the FDA.[9] While the FDA provides a form of "training" and licensure oversight, there is no corollary to the confidentiality and privilege requirement placed on mental health providers.

Chatbots as well as other mental health apps do not have any confidentiality requirements placed upon them, despite the myriad of federal and state statutes.[10] While these tools are subject to the

---

2. Heung-Yeung Shum, Xiaodong He & Di Li, *From Eliza to XiaoIce: Challenges and Opportunities with Social Chatbots*, 19 FRONTIERS INFO. TECH. & ELECTRONIC ENGINEERING 10, 12 (2018).

3. *See infra* Section II.A.

4. *See, e.g.*, Romeo, *supra* note 1 (discussing the creation of a chatbot therapist).

5. *See Types of Mental Health Professionals*, NAMI: NATIONAL ALLIANCE ON MENTAL ILLNESS, https://www.nami.org/learn-more/treatment/types-of-mental-health-professionals (last updated Aug. 2017).

6. *See, e.g.*, Allison N. Winnike & Bobby Joe Dale III, *Rewiring Mental Health: Legal and Regulatory Solutions for the Effective Implementation of Telepsychiatry and Telemental Health Care*, 17 HOUS. J. HEALTH L. & POL'Y 21, 69-76 (2017) (providing a sample of requirements placed on mental health professionals solely as applies to telepsychiatry and telemental health).

7. William J. Winsdale & Judith Wilson Ross, *Privacy, Confidentiality, and Autonomy in Psychotherapy*, 64 NEB. L. REV. 578, 622 (1985).

8. For a discussion of FDA Oversight, see Part III. A "medical device" is broadly defined as a device intended to provide treatment or diagnosis of a disease. 21 U.S.C. § 321(h) (2018).

9. *See, e.g.*, WOEBOT, https://woebot.io (last accessed May 1, 2018).

10. *See* Molteni, *supra* note 1. Molteni specifically pointed out that "[Woebot] only talks to you through Facebook Messenger. Facebook's services aren't HIPAA compliant, but in this case that wouldn't matter anyway. Because

Federal Trade Commission Act ("FTCA") and similar state consumer protection laws, these laws place no affirmative obligations on apps to maintain information as confidential. Instead, they require only notice to the consumer of the intended usage and disclosure of information.[11] Further, many of the existing general health information confidentiality obligations, such as the Health Information Portability and Accountability Act ("HIPAA"), do not apply to these tools, because they do not engage in certain types of electronic transactions.[12] Moreover, narrower health information confidentiality statutes, such as the Substance Abuse and Mental Health Services Administration ("SAMHSA") regulations and state mental health confidentiality requirements, either focus on certain types of providers or do not consider or encompass apps.[13]

Users engaging with these apps disclose information similar to information disclosed during a therapy session, yet their information is not afforded the same protection. Therapy, counseling, and other types of mental health treatment and assistance leverage techniques such as Cognitive Behavioral Therapy ("CBT").[14] CBT is a form of treatment that permits patients to work on their own modes of thinking through discussion and the development of coping skills.[15] When speaking with mental health professionals, who employ similar techniques to these tools, patients are afforded substantial confidentiality protections.[16] These protections stem from concerns about the unique nature of psychotherapy.[17] Users may be hesitant to disclose information necessary to obtain treatment due to concerns of embarrassment, shame, or guilt; or, users may be unable to access treatment.[18]

Given the unique nature of the information provided and the analogy to traditional therapy, this Article recommends the adoption of new legislation to limit the use and disclosure of information received by software-based therapy technologies. Part II provides an

---

Woebot isn't a licensed medical provider, any conversations with it aren't protected by medical data privacy and security law in the first place." *Id.*

11. *See infra* Section IV.A.

12. *See infra* Section IV.B.

13. *See infra* Section IV.C.

14. *See, e.g.*, AM. PSYCHOLOGICAL ASS'N, PTSD CLINICAL PRACTICE GUIDELINE, WHAT IS COGNITIVE BEHAVIORAL THERAPY?, http://www.apa.org/ptsd-guideline/patients-and-families/cognitive-behavioral.pdf (last accessed May 1, 2018).

15. *Id.*

16. *See, e.g.*, D.C. CODE §7-1201.02 (2018).

17. *See, e.g.*, Winsdale & Ross, *supra* note 7.

18. *Id.* at 641.

overview of chatbots and other software-based therapies. Part III reviews the framework under which the FDA regulates medical devices and showcases whether and how the FDA can regulate these technologies as medical devices. Part IV evaluates current federal and state laws applicable to healthcare apps, determining that the apps discussed herein are not subject to such regulations. Part V evaluates the need for additional regulation. It begins by using the factors considered by the Supreme Court in *Jaffee v. Redmond* as guideposts for evaluating whether confidentiality regulations should be created and determines that confidentiality regulations are appropriate.[19] It then considers counterarguments against the creation of such regulations, deeming them untenable. It then proposes a regulatory oversight framework, using principles from the FDA device framework as well as the FTCA and HIPAA privacy frameworks. Part VI concludes that a new regulatory framework for these apps solves this regulatory gap, but the issue of confidentiality is likely to recur in other emerging technologies that will pose similar questions.

II. CHATBOTS: MODERNIZING AN OLD TECHNOLOGY

Simply put, a chatbot is "a software program that interacts with users using natural language."[20] Chatbots leverage algorithms to mimic a conversation "between a human user and a computer using natural language."[21] This technology permits users to interact with computers in a way that is "natural" for them and is analogous to human conversation.[22] Chatbots historically have been associated with providing therapy and evaluating mental health issues, but have also recently become tools used in e-commerce; in a variety of sales, support, and assistant functions;[23] and for education and training purposes.[24]

19. Jaffee v. Redmond, 518 U.S. 1 (1996)

20. Bayan Abu Shawar & Eric Atwell, *Chatbots: Are they Really Useful?*, 22 LDV FORUM 29, 29 (2007).

21. *Id.* at 30.

22. *Id.* at 29.

23. *Id.* at 30; *see also id.* at 43-45 (discussing a variety of different recent uses of chatbots in this area).

24. *Id.* at 30; *see also id.* at 40-43 (discussing the use of chatbots in education and training purposes).

A. From ELIZA to Alexa

Joseph Weizenbaum created the first chatbot in 1966 when he created ELIZA.[25] Weizenbaum created ELIZA "to emulate a psychotherapist in clinical treatment."[26] The rules behind ELIZA were simple: ELIZA would search the text entered by a user for a specific keyword and would then use specific rules to provide a response based on the keyword.[27] If a user did not enter a keyword, then the rules would respond with a default phrase, such as "Very interesting. Please go on." or "Can you think of a special example?"[28] Some of the sample text from an initial discussion with ELIZA is as follows:

> ELIZA: Your boyfriend made you come here?
>
> Human: He says I'm depressed much of the time.
>
> ELIZA: I am sorry to hear that you are depressed.
>
> Human: It's true. I am unhappy.
>
> ELIZA: Do you think coming here will help you not to be unhappy?
>
> Human: I need some help, that much seems certain.
>
> ELIZA: What would it mean to you if you got some help?[29]

The initial technology behind ELIZA was necessary to determine the most important words, identify the context, and respond appropriately.[30]

---

25. *See, e.g.*, *id.* (discussing the history of chatbots and chatbot architectures); Joseph Weizenbaum, *ELIZA – A Computer Program for the Study of Natural Language Communication Between Man and Machine*, 9 COMM. ACM 36 (1966).

26. Shawar & Atwell, *supra* note 20, at 35. Some have stated that Weizenbaum's intent was to parody a psychotherapist. John Markoff, *Joseph Weizenbaum, Famed Programmer, Is Dead at 85*, N.Y. TIMES (Mar. 13, 2018), https://www.nytimes.com/2008/03/13/world/europe/13weizenbaum.html ("The software parodied the part of a Rogerian therapist, frequently reframing a client's statements as questions.").

27. Shawar & Atwell, *supra* note 20, at 35.

28. *Id.* at 35-6.

29. Weizenbaum, *supra* note 25 (emphases omitted).

30. Shawar & Atwell, *supra* note 20, at 37.

After ELIZA, Kenneth Colby developed PARRY in 1972.[31] Colby, a psychiatrist, wanted to develop a chatbot that mimicked a paranoid schizophrenic.[32] PARRY used an operating framework similar to ELIZA—attempting to determine keywords or phrases—but consisted of an additional module that "size[d] up the current state of the interview and decide[d] which linguistic actions to perform."[33] Thus, PARRY had a better understanding of the conversation and could respond accordingly.[34] However, PARRY's focus was not in assisting with mental health therapy; it aimed instead to showcase how the technology could be used to mimic someone with mental health issues.[35]

Little work had been done at the intersection of chatbots and therapy until the early 1990s.[36] In 1992, Creative Labs created a chatbot as part of its Sound Blaster product called Sound Blasting Acting Intelligent Text to Speech Operator ("SBAITSO").[37] Dr. Sbaitso provided responses similar to those of a therapist or psychologist, such as "WHY DO YOU FEEL THAT WAY?"[38] However, Creative Labs focused on creating text-to-speech functionality and extending the scope of chatbots rather than the provision of therapy.[39] Three years later, in 1995, Richard Wallace

---

31. Shum et al., *supra* note 2, at 12.

32. *Id.*; *see also* KENNETH COLBY, ARTIFICIAL PARANOIA: A COMPUTER SIMULATION OF PARANOID PROCESSES (1st ed. 1975) (discussing how to simulate paranoia).

33. Jason Hutchens, How to Pass the Turing Test by Cheating 9 (Apr. 23, 1996) (unpublished manuscript), *available at* https://www.csee.umbc.edu/courses/471/papers/hutchens.pdf.

34. *Id.* ("PARRY has knowledge about the conversation so far, and its current state of mind. If it is provoked it will get angry, and its responses to the interview will change appropriately.")

35. *Id.* Notably, PARRY passed the Turing Test. Shum et al., *supra* note 2, at 12. The Turing Test, created by Alan Turing, is a test used to determine whether a computer program is intelligent, or, more specifically, whether an individual can differentiate between a human and a machine. Hutchens, *supra* note 33, at 2-3.

36. While little work had been done until the 1990s, some have cited the creation of "Jabberwacky" in the 1980s as the next step in the evolution of chatbots. *See, e.g.*, Jo Twist, *Chatbot Bids to Fool Humans*, BBC NEWS (Sept. 22, 2003), http://news.bbc.co.uk/2/hi/technology/3116780.stm. Jabberwacky was intended for entertainment purposes, rather than for mental health purposes. *Id.*

37. *Dr. Sbaitso*, CLASSICRELOAD, https://classicreload.com/dr-sbaitso.html (last accessed Apr. 30, 2018).

38. *Id.*

39. *Dr. Sbaitso Will Listen to You*, GIZMODO (Apr. 28, 2006), https://gizmodo.com/170401/dr-sbaitso-will-listen-to-you. As one user put it:

> Doctor Sbaitso was meant to be the player's 'psychiatrist,' able to converse to-and-fro both with onscreen text and a horrendously off-kilter

developed the Artificial Language Internet Computer Entity ("ALICE").[40] ALICE leveraged a similar framework to that of ELIZA but used simpler programming.[41] Unlike its predecessor ELIZA, ALICE has survived the test of time as an open-source chatbot.[42]

Chatbot technology continued to expand in the 2000s, being used for entertainment and the creation of "assistants." The increased use of the internet and messaging systems in the early 2000s created an opportunity for a company called ActiveBuddy, which intended to lead the way in artificial intelligence.[43] ActiveBuddy wanted to create "bots that got to know their users, and could relay information instantly, in a conversational manner."[44] One such bot was called SmarterChild.[45] SmarterChild's creators believed users engaged with SmarterChild because SmarterChild could piece together prior thoughts or pieces of information to draw users into conversations and alleviate loneliness.[46] In fact, SmarterChild's ability to have a "personality" and create authentic responses arguably created a level of trust and intimacy akin to a relationship.[47] Though SmarterChild was ultimately taken offline, its founders believed it was ahead of its time.[48]

In the wake of SmarterChild, chatbots have been used predominantly as digital assistants, such as Siri and Alexa. These modern chatbots help individuals perform simple tasks.[49] However,

---

> voice coming through the speakers. Though some would consider the game to have included some degree of artificial intelligence, it really didn't: Doctor Sbaitso couldn't understand a thing, and all of his responses were essentially rephrasings of whatever you said, mixed with a few key phrases that would illicit [sic] more surprising answers.

Id.

40. Shum et al., *supra* note 2, at 3.

41. Vibhor Sharma et al., *An Intelligent Behaviour Shown by Chatbot System*, 3 INT. J. NEW TECH. & RES. 52, 53 (2017).

42. Shum et al., *supra* note 2, at 3. ALICE won a number of prizes in the early 2000s and continued to be used as of 2009. *Id.*

43. Ashwin Rodrigues, *A History of SmarterChild*, VICE: MOTHERBOARD (Mar. 16, 2016, 5:00 AM), https://motherboard.vice.com/en_us/article/jpgpey/a-history-of-smarterchild.

44. *Id.*

45. *Id.*

46. Robert Hoffer, *The Trouble With Bots: A Parent's Musings on SmarterChild*, VENTUREBEAT (June 15, 2016), https://venturebeat.com/2016/06/15/the-trouble-with-bots-a-parents-musings-on-smarterchild.

47. *Id.*

48. *Id.*

49. Shum et al., *supra* note 2, at 3. As Shum et al. state, "[i]n the past several years, a tremendous amount of investment has been made to developing

unlike SmarterChild, these types of apps have no memory, have no personality, and do not create the same level of intimacy or trust.[50]

B. Woebot, Wysa, and Mental Health Chatbots

Developers, entrepreneurs, and clinicians have recognized that the U.S. faces a mental health problem that can potentially be solved through emerging technologies.[51] They have thus leveraged chatbots to simulate CBT, a technique commonly used by mental health professionals.[52] Currently, at least two apps are available to consumers for mental health chat and support: Woebot and Wysa.[53]

Woebot began as a study undertaken by professors in the school of psychiatry at Stanford University.[54] The professors acknowledged the potential for text-based CBT, but noticed that in spite of a number of potential apps, "none of them were available commercially."[55] The team at Stanford designed the bot to act as a "choose your own adventure self-help book" based on clinical decision-making and CBT with tailored, empathic responses.[56] The study found that chatting with Woebot reduced symptoms of depression, and some study participants characterized Woebot as "a friend" or "a fun little dude."[57]

Wysa was created in a similar manner to Woebot.[58] The inventors wanted to use AI to detect depression, as they recognized potential access and stigma hurdles preventing individuals from

---

intelligent personal assistants (IPAs) such as Apple's *Siri*, Microsoft's *Cortana*, *Google Assistant*, *Facebook M*, and Amazon's *Alexa*." *Id.*

50. Hoffer, *supra* note 46.

51. Natasha Mathur, *Digital Health: The Next Frontier in Mental Health* Care, CHI. POL'Y REV. (Jan. 26, 2018), http://chicagopolicyreview.org/2018/01/26/digital-health-the-next-frontier-in-mental-health-care.

52. Nidhi Singh, *Are You Depressed? Talk to these Chatbots*, ENTREPRENEUR INDIA (June 9, 2017), https://www.entrepreneur.com/article/295601.

53. *Id.*

54. Kathleen Kara Fitzpatrick, Alison Darcy & Molly Vierhile, *Delivering Cognitive Behavioral Therapy to Young Adults with Symptoms of Depression and Anxiety Using a Conversational Agent (Woebot): A Randomized Controlled Trial*, 4 J. MED. INTERNET RES. MENTAL HEALTH 19 (2017).

55. *Id.*

56. *Id.*

57. *Id.*

58. *Questions most often asked by our users*, WYSA, https://www.wysa.io/faq (last accessed May 1, 2018) (noting that "Wysa is the result of a year-long co-design effort between a 15-people team of psychologists, designers, developers and over 500,000 users").

seeing a therapist.[59] One of the inventors estimated that India has around five thousand therapists and psychiatrists for a population of 1.3 billion, and that patients have to wait around one year to see a psychiatrist.[60] The early team created Wysa as a side experiment, and it continued to grow and develop from there.[61] Individuals have written to the team at Wysa saying that it saved their lives.[62] While little is known about how these apps function due to their proprietary nature, they use similar technologies to those of their predecessors, albeit likely in a more advanced format with modern algorithms.

While the types of technologies described above[63] appear beneficial, there are a number of questions raised by these apps. Some may ask whether these tools are intended to replace existing mental health professionals.[64] Others may wonder about their safety and efficacy.[65] While the apps raise a number of questions or concerns, fundamentally, the apps provide services akin to mental health professionals and involve users disclosing information they may consider sensitive. Because of this sensitivity, the efficacy of the apps is closely tied to the question of how the apps handle the privacy—or more aptly, confidentiality—of information provided by users.[66]

---

59. Eric Wallach, *An Interview with Jo Aggarwal, Co-Inventor of Wysa*, POLITIC (Mar. 28, 2018), http://thepolitic.org/an-interview-with-jo-aggarwal-co-inventor-of-wysa/.

60. *Id.*

61. *Id.*

62. *Id.* Jo Aggarwal specifically mentioned a "13-year old girl who wrote to [Wysa] and said that she tried to commit suicide, and Wysa was helping her hold on to life."

63. Though the focus of this article is narrow—specifically looking at chatbots—other developers have created mobile apps leveraging cognitive behavioral therapy. Examples of these include Pacifica, http://www.thinkpacifica.com and Happify, https://www.happify.com/.

64. Wallach, *supra* note 59 (noting that the creators of Wysa never intended it to replace mental health professionals).

65. Amy Ellis Nutt, *'The Woebot will see you now'-the rise of chatbot therapy*, WASH. POST (Dec. 3, 2017), https://www.washingtonpost.com/news/to-your-health/wp/2017/12/03/the-woebot-will-see-you-now-the-rise-of-chatbot-therapy (noting that a member of the American Psychiatric Association had concerns about whether these tools were effective); *see also* Theodore Lee, *Recommendations for Regulating Software-based Medical Treatments: Learning from Therapies for Psychiatric Conditions*, 73 FOOD & DRUG L.J. 66 (2018) (discussing the issue of safety and effectiveness in digital therapies).

66. Molteni, *supra* note 1. Scholars have debated the nature of privacy and confidentiality. *See, e.g.*, Winsdale & Ross, *supra* note 7, at 593-97 (1985) (discussing the nature of privacy and confidentiality and distinctions therein). Some scholars highlight the distinction between an "invasion" or "loss" of privacy, in which an individual must disclose something otherwise private for treatment,

III. CHATBOT & SOFTWARE APP REGULATORY OVERSIGHT

Though this Article does not deal with the question of whether or how the FDA should regulate software-based therapy as medical devices,[67] it is helpful to understand the framework of FDA oversight in considering how to craft confidentiality requirements. According to the Food, Drug & Cosmetic Act, the FDA provides oversight for medical devices, or, as the statute defines devices, any "instrument, apparatus, implement, machine, contrivance, . . . or other similar component, part, or accessory, which is . . . intended for use in the diagnosis of disease or other conditions or in the cure, mitigation, treatment or prevention of disease."[68] Initially, the FDA provided oversight of medical devices solely through its adulteration and misbranding provisions.[69] In 1976, the FDA began to regulate the safety and efficacy of medical devices.[70]

---

and confidentiality, which arises from a relationship, conduct, and context in which society (and the courts) recognize information to be maintained in secrecy and not further disclosed. *Id.* at 594. Recently, some have conflated the concept of confidentiality with privacy by adopting a theory of quasi-property. *See* Lauren Henry Scholz, *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113, 1123-24 (2016) (advocating for a theory of quasi-property looking at context, conduct, and relationship in terms of privacy). *Compare id.* (setting forth privacy as an evaluation of context, conduct, and relationship) *with* Winsdale & Ross, *supra* note 7, at 594-5 (discussing confidentiality as status afforded to data based on the nature thereof, based on an agreement or understanding, and based on certain specific relationships).

67. For a discussion of suggestions on how the FDA should provide oversight to software-based therapy, see, for example, Lee, *supra* note 65.

68. 21 U.S.C. § 321(h). The definition of "device" has two additional statutory components. Something may be considered a device if it is:

> Recognized in the official National Formulary, or the United State Pharmacopeia, or any supplement to them; . . .
>
> Intended to affect the structure or any function of the body of man or other animal and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary purpose . . . .

Some have noted the breadth with which the FDA could or has interpreted "device." *See, e.g.*, Lucas Mearian, *FDA eyes regulation of wireless networks at clinics, hospitals*, COMPUTERWORLD (Jan. 10, 2011), https://www.computerworld.com/article/2512134/healthcare-it/fda-eyes-regulation-of-wireless-networks-at-clinics–hospitals.html.

69. *See* United States v. Bacto-Unidisk, 394 U.S. 784, 784-85 (1969) ("If, on the other hand, the article is merely a 'device' under the Act, it is subject only to the misbranding and adulteration proscriptions of the Act and does not have to be pre-tested before marketing.").

70. Medical Device Amendments of 1976, Pub. L. No. 94-295, 90 Stat. 239 (1976). For more information on the methods by which the FDA regulates medical

In 1989, the FDA promulgated a guidance document discussing how it intended to regulate software under this schema.[71] The FDA guidance focused on two different groups of devices: those it would not regulate and those over which it would exercise enforcement discretion.[72] The FDA clarified that it would not regulate computer functions not intended for use in diagnosis or in cure, mitigation, treatment, or prevention of disease and would not regulate computer functions that were a component, part, or accessory of another medical device already subject to FDA oversight.[73] The FDA also created four different categories of software for which it would exercise its enforcement discretion: (1) a general purpose item used in healthcare;[74] (2) a computer product used by the creator for its own practice;[75] (3) a computer product used for teaching or non-clinical research;[76] or (4) computer products that permit human intervention.[77] This guidance reiterated the definition of "device."[78]

The FDA did not provide much further guidance on how it would regulate software functionality until it promulgated a proposed guidance document for mobile medical applications in 2011.[79] In this guidance document, the FDA focused narrowly on two distinct classes of technologies: The FDA sought to provide

---

devices and the classification of such devices, see, for example, Vincent J. Roth, *The mHealth Conundrum: Smartphones & Mobile Medical Apps – How Much FDA Medical Device Regulation is Required?*, 15 N.C. J.L. & TECH 359, 373-381 (2013) (discussing how the FDA classifies and reviews medical devices).

71. Draft FDA Policy for the Regulation of Computer Products, 1989 WL 1178702, at *1 (Nov. 13, 1989)

72. *Id.*

73. *Id.* at *1-2.

74. *Id.* at *2. These items would be "a product that is not labeled or promoted for medical uses but which, by virtue of its application in health care, meets the definition of a medical device." For example, a personal computer displaying lab values or a database management system, with no medical claims, would meet this exemption.

75. *Id.* Though this may be exempt from regulation as it is not provided for in interstate commerce, the FDA did permit practitioners to provide the software "without charge to other similar medical facilities" without requiring regulation.

76. *Id.* The FDA believed that this exemption would be limited to those "research and development efforts which have not progressed to the stage of human experimentation."

77. *Id.* Today, such systems would likely constitute clinical decision support systems, and be subject to the FDA's guidance regarding such systems. *See* Clinical and Patient Decision Support Software: Draft Guidance for Industry and Food and Drug Administration Staff, 82 Fed. Reg. 57987 (proposed Dec. 8, 2017) [hereinafter FDA Decision Support Software Guidance].

78. *See* 21 U.S.C. § 321(h) (2018).

79. Mobile Medical Applications: Draft Guidance for Industry and Food and Drug Administration Staff, 76 Fed. Reg. 43689, 43689 (proposed July 21, 2011).

oversight over devices that were "used as an accessory to a regulated medical device" and those that "transform[] a mobile platform into a regulated medical device."[80] The agency did not address new and emerging technologies, but relied on its definitions and exercising enforcement discretion over other devices.[81]

The FDA continued to wrestle with the question of how to regulate software as medical devices through additional guidance documents.[82] Ultimately, the FDA adopted a three-tiered approach to regulatory oversight. First, the FDA created a group of mobile apps or mobile app functionalities that would not be considered medical devices.[83] This category included reference materials, educational tools, and general office or general purpose software.[84] Second, the FDA created a group of mobile apps or functionalities that could be considered devices, but for which the FDA would "exercise enforcement discretion for these mobile apps because they pose lower risk to the public."[85] Notably, this group would include "[m]obile apps that help patients with diagnosed psychiatric conditions . . . maintain their behavioral coping skills," or "that display, at opportune times, images or other messages for a substance abuser who wants to stop addictive behavior."[86] The final group would be those subject to FDA oversight and would "transform a mobile platform into a regulated medical device,"[87] would "connect to an existing device . . . for purposes of controlling its operation, function, or energy source,"[88] or would be "used in active patient monitoring or analyzing patient-specific medical device data."[89]

Congress decided to clarify the scope of the FDA's oversight in this realm as part of the 21st Century Cures Act of 2017.[90] Congress

---

80. *Id.*

81. *Id.*

82. The FDA promulgated additional guidance documents in 2013 and 2015. *See* Nathan Cortez, *The Mobile Health Revolution*?, 47 U.C. DAVIS L. REV. 1173, 1221-24 (2014) (discussing the 2013 Mobile Medical Application Guidance).

83. U.S. FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 20 (Feb. 9, 2015), https://www.regulations.gov/document?D=FDA-2011-D-0530-0110 [hereinafter FINAL MMA GUIDANCE].

84. *Id.* at 20-22.

85. *Id.* at 23.

86. *Id.* at 23-24.

87. *Id.* at 27.

88. *Id.* at 28.

89. *Id.* at 29.

90. 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016). In addition to clarifying the scope of oversight, the 21st Century Cures Act attempted

exempted certain types of software functionality from the definition of "device," leaving the FDA the ability to regulate other forms of functionality existing in a single app.[91] Congress identified five distinct types of functionality that would be exempt from the definition of device: those used "A) for administrative support of a health care facility";[92] "B) for maintain[ing] or encouraging a healthy lifestyle . . . unrelated to . . . a disease or condition";[93] C) for acting as electronic patient records;[94] D) for certain functions related to laboratory tests and clinical data;[95] and E) for providing medical information or "recommendations to a health care professional," or for "enabling [a] health care professional to independently review the basis for such recommendations."[96] However, Congress did not entirely exempt the third, fourth, and fifth categories from FDA oversight, permitting the Secretary of Health and Human Services ("HHS") to regulate software functionality under certain circumstances.[97]

In response to the 21st Century Cures Act, on December 8, 2017, the FDA issued additional guidance documents pertaining to the oversight and review of software functions.[98] While the first two are

---

to provide new, quicker routes to market, as well as avenues for clearance and approval for devices. *See, e.g.*, Sarah Faulkner, *How the 21st Century Cures Act Will Affect Medical Devices*, MASSDEVICE (Dec. 8, 2016), https://www.massdevice.com/21st-century-cures-act-will-affect-medical-devices.

91. 21 U.S.C. § 360j(o)(2) (2018) (allowing the FDA to regulate other portions of a piece of software as a device and clarifying that the exempted section shall not constitute such a device).

92. 21 U.S.C. § 360j(o)(1)(A).

93. *Id.* at § 360j(o)(1)(B).

94. *Id.* at § 360j(o)(1)(C). The definition of electronic patient records seems to focus solely on electronic patient records under the Meaningful Use program and not to include personal health records. For a discussion of the Meaningful Use program and certification, see, for example, Joseph D. Szerejko, Note, *Reading Between the Lines of Electronic Health Records: The Health Information Technology for Economic and Clinical Health Act and Its Implications for Health Care Fraud and Information Security*, 47 CONN. L. REV. 1103, 1109-19 (2015); Nicolas P. Terry, *Certification and Meaningful Use*: *Reframing Adoption of Electronic Health Records as a Quality Imperative*, 8 IND. HEALTH L. REV. 43, 49-61 (2011).

95. *Id.* at § 360j(o)(1)(D).

96. *Id.* at § 360j(o)(1)(E).

97. *Id.* at § 360j(o)(3). To exercise discretion and oversight over the software, the Secretary would need to determine whether the "software function would be reasonably likely to have serious adverse health consequences" and promulgate a final order identifying the function. *Id.*

98. *Guidances with Digital Health Content*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/MedicalDevices/DigitalHealth/ucm562577.htm (last updated Aug. 30, 2018).

not relevant to this Article,[99] the third provides interesting insight into the FDA's continued oversight of software functionality.[100] The guidance document, *Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act*, discusses the FDA's existing software policies and reiterates the Cures Act's focus on the software *function*, rather than the entire application.[101] The FDA deferred to its prior guidance for determining whether something constitutes a "general wellness product,"[102] which it defined as: (1) "an intended use that relates to maintaining or encouraging a general state of health or a healthy activity," or (2) "an intended use that relates the role of health lifestyle with helping to reduce the risk or impact of certain chronic diseases and conditions."[103] With respect to the first category, the FDA provided examples of software that would qualify under the general wellness category, including "software with health lifestyle management, such as . . . relaxation or stress management, mental acuity, self-esteem, [or] sleep management . . . when not related to the diagnosis, cure, mitigation, prevention or treatment of a disease or condition."[104]

Thus, when looking at the FDA's oversight ability, it is unclear at this point whether the types of mental health tools discussed in

---

99. One document focused on clinical decision support. *See* FDA DECISION SUPPORT SOFTWARE GUIDANCE, *supra* note 77. It discussed how the FDA would interpret some of the clinical decision support items referenced previously. *Id.* at 6. The other document focused on the adoption of principles related to software as a medical device. U.S. FOOD & DRUG ADMIN., SOFTWARE AS A MEDICAL DEVICE (SAMD): CLINICAL EVALUATION - GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Dec. 8, 2017), https://www.regulations.gov/document?D=FDA-2016-D-2483-0021.

100. U.S. FOOD & DRUG ADMIN., CHANGES TO EXISTING MEDICAL SOFTWARE POLICIES RESULTING FROM SECTION 3060 OF THE 21ST CENTURY CURES ACT: DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Dec. 8, 2017), https://www.regulations.gov/document?D=FDA-2017-D-6294-0002 [hereinafter CURES GUIDANCE].

101. *Id.* at 7. Notably, this would suggest that portions of an application would or could be regulated by the FDA, while other portions of the application may not be subject to FDA oversight.

102. U.S. FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES - GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION (July 29, 2016), https://www.regulations.gov/document?D=FDA-2014-N-1039-0016. This guidance document is currently under review by the FDA. *Id.* at 1.

103. CURES GUIDANCE, *supra* note 100, at 8. The second category of intended uses must not only relate to the condition, but it must also be "well understood and accepted that healthy lifestyle choices may play an important role in health outcomes for the disease or condition." *Id.*

104. *Id.*

this Article will be viewed as medical devices subject to the FDA approval or clearance process. The recently issued draft guidance suggests that as long as chatbots are not targeted to treat or diagnose specific conditions, but are merely there to provide "chat" or "support," they would not be subject to FDA oversight.[105] However, the line at which "chat" or "support" ends and "treatment" begins is unclear.[106] Even if chatbots were subject to FDA approval, the FDA's focus is safety and efficacy,[107] which includes certain security controls for devices.[108] FDA oversight will not solve the question of confidentiality requirements.[109]

IV. CHATBOT CONFIDENTIALITY: THE APPLICABILITY OF U.S. CONFIDENTIALITY LAWS

While the FDA may provide some degree of oversight of the safety and efficacy of chatbot apps, existing confidentiality laws provide no restrictions on the ability of these technologies to use or disclose information obtained from users. The U.S. confidentiality framework applicable to these technologies can be thought of in three different categories. The first and broadest category consists of federal and state consumer protection laws that ensure that businesses as well as apps inform a consumer of how they will use and disclose a consumer's information.[110] So long as the entity does not engage in an "unfair or deceptive" practice with respect to the

105. This is not only indicated through the FDA's recent guidance document, but also through the FDA's history of focusing on "intended use." *See, e.g.*, Gary E. Gamerman, Note, *Intended Use and Medical Devices: Distinguishing Nonmedical "Devices" from Medical Devices under 21 U.S.C. 321(h)*, 61 GEO. WASH. L. REV. 806 (1993) (discussing the history and focus of the FDA on intended use, as an extension of the definition of device).

106. This is indicated by the different types of examples offered by the FDA in the prior guidance document. *See* FINAL MMA GUIDANCE, *supra* note 83 (indicating the difficulty in determining when something constitutes a "device" for purposes of oversight and providing the FDA discretion in the determination).

107. Roth, *supra* note 70, at 362.

108. *FDA Fact Sheet: The FDA's Role in Medical Security*, U.S. FOOD AND DRUG ADMIN. (last visited Apr. 30, 2018), https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf (noting that device manufacturers must address cybersecurity risks as part of the FDA quality system regulations (QSRs)).

109. *Id.* As noted in the fact sheet, the FDA provide some degree of *security*, but since the focus is on the device, the main focus is on safety and efficacy. *Id.* The FDA could broaden its definitions of safety and efficacy to encompass mental health tools; however, this seems unlikely.

110. *See infra* Section IV.A.

information, a business or app can essentially do whatever it chooses with the information.[111]

The second category consists of federal and state general health confidentiality laws, which prohibit certain uses and disclosures of information. Generally, these laws only apply to licensed healthcare providers or licensed healthcare providers billing insurance (or other types of healthcare transactions).[112] The third category comprises federal and state specific health confidentiality laws, which focus on certain types of healthcare providers or certain types of health conditions, to which additional absolute prohibitions on disclosure attach.[113] Though there are a number of laws focusing on health information confidentiality with heightened restrictions on disclosures for mental health, none apply to chatbots, chatbot apps, or similar technology.

A. Consumer Privacy Laws

The broadest laws affecting individual privacy have, in fact, nothing to do with privacy, but rather focus on consumer protection. Congress created the Federal Trade Commission ("FTC") in 1914 to "protect consumers and promote competition," predominantly through enforcement of antitrust statutes.[114] This initial antitrust focus meant that the agency was charged with looking only at actions that harmed competitors.[115] However, Congress later broadened the agency's focus to encompass consumer harm, by looking at "unfair or deceptive acts or practices as well as 'unfair methods of competition.'"[116] This expansion of authority allowed the FTC to investigate almost any company.[117]

---

111. *See infra* Section IV.A. *See also* 15 U.S.C. § 45 (2018).

112. *See infra* Section IV.B.

113. *See infra* Section IV.C.

114. *Our History*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/our-history (last visited Apr. 30, 2018). *See also* Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 231 (2017).

115. Pardau & Edwards, *supra* note 114, at 231-32.

116. *Id.* at 232. Congress did not define "unfair or deceptive acts" as part of the legislation, largely leaving the agency to interpret what this was and how to enforce. *See* J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall and Resurrection*, FED. TRADE COMM'N (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

117. Pardau & Edwards, *supra* note 114, at 233. Some of the initial enforcement actions by the FTC were brought against funeral homes and vending machine companies. *Id.*

In the 1990s, the FTC turned its attention to new internet technologies and what role, if any, it would have in regulating these technologies.[118] The FTC initially advocated for self-regulation.[119] It believed that the changing nature of technology required a hands-off approach, thus recommending "self-regulation [as] the least intrusive and most efficient means to ensure fair information practices."[120] Despite this position, it advocated for congressional action to protect children given their status as a potentially vulnerable population.[121]

Regardless of its position on self-regulation, the FTC could still exercise its authority by investigating privacy policies that were "unfair or deceptive."[122] "Unfair or deceptive" in this case meant that the business failed to notify a consumer of a use or disclosure of data.[123] The FTC's first enforcement action against an internet business involved a company called GeoCities in 1998.[124] GeoCities provided websites and email addresses for users on both a paid and free basis. GeoCities requested that users provide information in mandatory and optional information fields, and the company represented to users that it would only provide the information to third parties when and if it received permission from the individual.[125] The FTC alleged that, in reality, GeoCities "sold, rented, or otherwise marketed or disclosed this information . . . to third parties who have used this information for purposes other than

---

118. FED TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 12 (July 1999), [hereinafter 1999 FTC REPORT]; *see also* Pardau & Edwards, *supra* note 114, at 235-237.

119. *Id.*

120. *Id.* at 6.

121. *Id.* at 4. This was in part due to a prior report to Congress. *Id.* The FTC's testimony in 1998 resulted in the enactment of the Children's Online Privacy Protection Act (COPPA). *Id.* at 5. For a history and critique of COPPA, see, for example, Lauren A. Matecki, *Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era*, 5 NW. J. L. & SOC. POL'Y 369 (2010).

122. *See* 15 U.S.C. § 45 (2018) ("[U]nfair or deceptive acts or practices in or affecting commerce [] are hereby declared unlawful.").

123. Michael A. Scott, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 131-133 (2008). In some instances, it has been unclear whether the action (or inaction) constitutes an "unfair" or "deceptive" act. *Id.* at 133 n.39.

124. Complaint, *In re* GeoCities, No. C-3850 (F.T.C. 1998), https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015cmp.htm [hereinafter GeoCities Complaint]; *see also* Scott, *supra* note 123, at 131 (noting that *In re* GeoCities was the first case involving internet privacy).

125. GeoCities Complaint, *supra* note 124, at ¶¶ 3, 12.

those for which members have given permission."[126] The FTC later issued a decision and order based on a consent agreement it had with GeoCities, which required GeoCities to make changes to its privacy notice and how it stored information, but did not include any monetary penalties.[127]

Since 1998, the FTC has engaged in over 200 actions regarding deceptive or unfair privacy practices,[128] including a fairly recent action involving an electronic health records provider, Practice Fusion ("PF").[129] PF offers electronic medical record services to healthcare providers and, as part of its business model, engages with patients directly through its patient portal.[130] PF asked patients for feedback regarding their healthcare provider and made this information publicly available.[131] The FTC noted that PF had updated its privacy policy to notify users that the information may be made public, but only after already making the information public under a prior privacy policy.[132] The FTC determined that PF's privacy policy was deceptive because it failed to notify users of the public disclosure prior to such disclosure.[133] The FTC has become one level of oversight for software-based and internet-based technologies, including those related to healthcare.

Though the majority of the FTC's focus is on whether the consumer has been given proper notice of how their information is used, the FTC has some additional responsibilities when dealing with personal health records and health information.[134] Personal health records ("PHR") provide consumers the ability "to store and organize medical information from many sources in one online location."[135] Though these records would likely be protected by general health information confidentiality requirements when in the

126. *Id.* at ¶ 14.

127. Decision and Order, *In re* GeoCities, No. C-3850 (F.T.C. 1998), https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do_.htm.

128. Beales, *supra* note 116.

129. Complaint, *In re* Practice Fusion, Inc., No. C-4591 (F.T.C. Aug. 15, 2016), https://www.ftc.gov/system/files/documents/cases/160816practicefusion cmpt.pdf [hereinafter Practice Fusion Complaint].

130. *Id.* at ¶¶ 3-4.

131. *Id.* at ¶¶ 5, 7.

132. *Id.* at ¶ 6.

133. *Id.* at ¶¶ 15-17.

134. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, §13407, 123 Stat. 269-70 (2009).

135. *Complying with the FTC's Health Breach Notification Rule*, FED. TRADE COMM'N (last updated Mar. 2019), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule [hereinafter *FTC Breach Notification Guidance*].

hands of health care providers,[136] the records would not be subject to those requirements when in the hands of consumers.[137] Congress required the FTC—in conjunction with HHS—to evaluate potential privacy, security, and breach notification requirements related to health information technology[138] and to promulgate a rule related to unauthorized access of a personal health record.[139] FTC promulgated the Health Breach Notification rule, which focused narrowly on "personal health record vendors, and their third party suppliers" and required PHR vendors to notify users in the event that an unauthorized individual accessed the user's record.[140] Congress recognized the important role the FTC plays in ensuring individual awareness of data privacy and security as well as the interplay between HHS and the FTC. However, the FTC's role has largely been to provide notice to consumers, rather than to provide or enforce affirmative confidentiality restrictions.

In addition to FTC protections at the federal level, state attorneys general ("AGs") enforce similar consumer protection statutes at the state level.[141] However, the degree of oversight and enforcement of these statutes is largely dependent on the individual AG. When dealing with new technology, the former AGs of California and New York have been particularly active.

Former California AG Kamala Harris focused on mobile application privacy activities and concerns, likely due to the substantial technology sector in California. AG Harris negotiated an agreement among multiple application developers—including Amazon, Google, Facebook, and Microsoft, among others—regarding privacy principles. These developers pledged "to educate developers about their obligations to respect consumer privacy."[142]

---

136. *See infra* Section IV.B (discussing general health information confidentiality statutes and applicability).

137. *See FTC Breach Notification Guidance*, *supra* note 135 ("You're not a vendor of personal health records if you're covered by HIPAA.").

138. *Id.*

139. *Id.*

140. *Id. See also* FTC Health Breach Notification Rule, 16 C.F.R. pt. 318 (2019).

141. *See, e.g.*, Henry N. Butler & Joshua D. Wright, *Are State Consumer Protection Acts Really Little FTC Acts?*, 63 FLA. L. REV. 163 (2011) (comparing the FTC Act to state consumer protection acts and noting the expansiveness of the latter).

142. Press Release, Office of Att'y Gen., Cal. Dep't of Justice, Attorney General Kamala D. Harris Secures Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012) https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

Following this meeting, Harris' office sent out up to one hundred letters of non-compliance in response to apps failing to implement an adequate privacy policy.[143] She also created privacy guidelines for mobile app developers.[144] These guidelines include using "special notices" to highlight unexpected uses or disclosures of information[145] and determining at the outset how data will be used or disclosed, and for what purposes.[146] While some have criticized her guidelines as being merely suggestions unrelated to the California Online Privacy Protection Act, the guidelines focus on ensuring transparency and adequacy of notice without the creation of specific protections.[147]

In addition to the work of former AG Harris, former New York AG Eric Schneiderman enforced violations of New York consumer protection laws against health-related mobile applications.[148] On March 23, 2017, AG Schneiderman entered into three settlements with individual or fetal heart-rate monitor manufacturers, which allegedly misled consumers.[149] While the fetal heart-rate monitor developer failed to obtain FDA approval,[150] the AG alleged the remaining developers did not provide users with a privacy policy,

143. Press Release, Office of Att'y Gen., Cal. Dep't of Justice, Attorney General Kamala D. Harris Notifies Mobile Developers of Non-Compliance with California Privacy Law (Oct. 30, 2012), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance.

144. Scott Reyburn, *California Attorney General's Office Releases Privacy Guidelines for Mobile App Developers*, ADWEEK (Jan. 10, 2013), http://www.adweek.com/digital/california-attorney-generals-office-releases-privacy-guidelines-for-mobile-app-developers; KAMALA D. HARRIS, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (Jan. 2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.

145. *See* HARRIS, *supra* note 144, at 12.

146. *Id.*

147. Reyburn, *supra* note 144.

148. Press Release, N.Y. State Office of the Att'y Gen., A.G. Schneiderman Announces Settlements with Three Mobile Health Application Developers for Misleading Marketing and Privacy Practices (Mar. 23, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-settlements-three-mobile-health-application-developers.

149. *Id.*

150. Assurance Of Discontinuance Under Executive Law Section 63, Subdivision 15, *In re* Matis, Ltd., Assurance No. 16-101 (Feb. 13, 2017), https://ag.ny.gov/sites/default/files/matis_aod_executed.pdf. Matis failed to obtain FDA approval, marketing itself as a fetal heart monitor without any evidence. *Id.* at 13-14. There was some discussion of a privacy policy and consumer perception, but the main focus was the alleged ability to monitor a fetal heart rate. *Id.*

nor did they notify users of the applicability of HIPAA.[151] Schneiderman suggested that the applicability of privacy laws—or lack thereof—is relevant and should be affirmatively stated to consumers.

When considering the applicability of state consumer protection laws, chatbot apps need to notify users of how their information is used and disclosed. There are no limitations on the permitted or prohibited types of uses or disclosures so long as the user is informed. While true, the settlements by the former New York AG suggest chatbots may need to determine and affirmatively state whether other laws, such as HIPAA, apply. However, this requirement only provides further notice to the user; it does not dictate how the app or app developer uses or discloses data.

B. General Health Information Confidentiality Laws

In addition to consumer laws, general health information confidentiality laws may apply to chatbot apps. These laws focus on information gained from users/patients, and they apply to any health or health-related information gathered. The federal health information confidentiality regulations are embodied in the HIPAA regulations,[152] and states have adopted legislation or regulation that is substantially similar in nature to HIPAA.[153]

HIPAA required Congress, or if Congress failed to act, the Secretary of HHS, to establish standards related to the privacy of individually identifiable health information.[154] As Congress did not enact any standards, HHS promulgated the initial Privacy Rule in 2000.[155] The initial Privacy Rule required only those entities covered

---

151. Assurance Of Discontinuance Under Executive Law Section 63, Subdivision 15 at 11-12, *In re* Cardiio, Inc., Assurance No. 16-173 (Jan. 23, 2017), https://ag.ny.gov/sites/default/files/cardiio_aod_executed.pdf; Assurance Of Discontinuance Under Executive Law Section 63, Subdivision 15 at 12-13, *In re* Runtastic GmbH, Assurance No. 16-174 (Jan. 31, 2017), https://ag.ny.gov/sites/default/files/runtastic_aod_executed_0.pdf.

152. 45 C.F.R. §§ 160 & 164 (2018).

153. INST. OF MED., IMPROVING THE QUALITY OF HEALTH CARE FOR MENTAL AND SUBSTANCE-USE CONDITIONS 405 (Nat'l Academies Press 2006) (discussing states that have privacy regimes akin to HIPAA).

154. Health Information Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264(a) (1996). The legislation required Congress to enact standards relating to privacy of individually identifiable health information within 36 months of the enactment of HIPAA. *Id.* at §264(c)(1). However, if Congress failed to do so, the legislation required the Secretary of HHS to promulgate rules within 42 months of the enactment of HIPAA. *Id.*

155. HHS Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000) [hereinafter HIPAA Privacy

by the legislation, i.e., a "covered entity," to comply with the privacy requirements.[156] Under the Privacy Rule, a covered entity could be a health plan,[157] a healthcare clearinghouse,[158] or a specific type of health care provider.[159] To be considered a health care provider under HIPAA, the individual or entity must be a provider of medical, mental, or health services, or otherwise "furnish[], bill[], or [be] paid for health care in the normal course of business."[160] The definition of "health care" is fairly broad and encompasses any "counseling, service, assessment, or procedure with respect to the physical mental condition, or functional status of an individual."[161]

In spite of this broad definition of health care provider, a health care provider is not a covered entity unless and until the health care provider engages in an electronic transaction covered by the rule.[162] HIPAA covers a number of different electronic transactions,[163] but generally, the electronic submission of insurance claims causes a health care provider to become a covered entity.[164] Thus, a health care provider can avoid becoming a covered entity by not accepting

---

Rule]. HHS drafted a proposed rule in 1999. HHS Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918 (proposed Nov. 3, 1999).

156. HIPAA Privacy Rule, *supra* note 155, at 82476-77.

157. *Id.* at 82478. A health plan is "an individual or group plan that provides, or pays the cost of medical care." 45 C.F.R. § 160.103 (2018).

158. HIPAA Privacy Rule, *supra* note 155, at 82477. A health care clearinghouse either transforms a standard transaction or standard data elements into a nonstandard format, or transforms a nonstandard transaction into a standard format. 45 C.F.R. § 160.103 (2018).

159. HIPAA Privacy Rule, *supra* note 155, at 82477-78.

160. 45 C.F.R. § 160.103 (2018).

161. *Id.* This is only a portion of the definition:

> *Health care* means care, services, or supplies related to health of an individual. Health care includes, but is not limited to, the following:
> Preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure of the body; and
> Sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

Id.

162. *Compare* 45 C.F.R. § 160.103 (defining health care provider) *with* 45 C.F.R. § 160.103 (defining a covered entity as a "health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter").

163. 45 C.F.R. § 160.103 (setting forth samples of transactions). The Secretary has the authority to create additional transactions by regulation. *Id.*

164. *See, e.g.*, 45 C.F.R. § 162.1101 (discussing the submission of health care claims).

or billing insurance, or by submitting (and having the payers accept) insurance claims in a non-electronic format.[165] Some mental health professionals, such as psychologists and psychotherapists, have begun to transition from accepting cash to billing insurance.[166] These providers were not previously subject to HIPAA, but they may be now.[167]

Assuming that HIPAA applies, HIPAA limits a covered entity's ability to use and disclose protected health information ("PHI").[168] Though the original, proposed HIPAA Privacy Rule suggested that a covered entity always obtain patient consent prior to any use or disclosure of patient information,[169] HHS abandoned this approach and now permits, but does not require, consent.[170] HHS then created a three-tiered structure for uses and disclosures: those for

---

165. *See* 45 C.F.R. § 160.103 (requiring a health care provider to engage in transactions to be considered a covered entity). The Secretary has the authority to create additional transactions by regulation. *Id.*

166. Sarah Varney, KAISER HEALTH NEWS, *Health Law Brings Changes in How Therapists Do Business* (Oct. 24, 2013), https://khn.org/news/health-law-changes-therapy-business/. *But see* April Demobsky, *Psychotherapists gravitate toward patients who can pay*, PBS NEWSHOUR (July 15, 2016, 10:10 AM EDT), https://www.pbs.org/newshour/health/psychotherapists-gravitate-toward-patients-can-pay (noting that mental health professionals tend to gravitate towards cash payment, with the majority of services going to the wealthy).

167. As to cash-pay practices, the assumption is these practices were not previously submitting health care claims, 45 C.F.R. § 162.1101, or other transactions, *id.* at § 160.103, and that they are now, thus satisfying the definition of covered entity and subjecting them to HIPAA. *Id.* at § 160.103.

168. The regulations define protected health information as "individually identifiable health information . . . [t]ransmitted by electronic media; [m]aintained in electronic media; or [t]ransmitted or maintained in any other form or medium." *Id.* at § 160.103. Individually identifiable health information is further defined by the regulations as:

> [A] subset of health information . . . [that]:
> Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
> That identifies the individual; or
> With respect to which there is a reasonable basis to believe the information can be used to identify an individual.

Id.

169. HIPAA Privacy Rule, *supra* note 155, at 82473-74.

170. *Id.*

which consent may be obtained,[171] those for which the patient must be provided an opportunity to opt out,[172] and those for which an authorization must be obtained.[173]

Under this framework, covered entities can use and disclose most protected health information to almost any healthcare entity for any health care-related purpose.[174] However, HIPAA does not permit the use and disclosure of psychotherapy notes without authorization.[175] Psychotherapy notes are "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record."[176] Although HHS originally required an authorization for everyone except the mental health professional that makes these notes,[177] the final Privacy Rule required the mental health professional to obtain an individual's

171. *See* 45 C.F.R. §§ 164.502(a)(1)-(3), 164.506(c), 164.512. Section 164.506(b)(1) expressly states that consent "may" be obtained. *Id.* at § 164.506(b)(1).

172. *Id.* at § 164.510. The uses and disclosures require the individual to be "informed in advance of the use or disclosure and [have] the opportunity to agree to or prohibit or restrict the use or disclosure." *Id.*

173. *Id.* at § 164.508. As noted in § 164.506, consent will not suffice to meet the requirement of an authorization. *See id.* at §164.506(b)(2). Uses and disclosures not authorized under the rule in either of the prior two sections require an authorization. *Id.* at § 164.508(a)(1). To be considered valid under HIPAA, an authorization must contain: 1) "a description of the information to be used or disclosed;" 2) "[t]he name or other specific identification(s) of the person(s), or class of persons, authorized to make the requested use or disclosure;" 3) "[t]he name or other specific identification of the person(s) . . . to whom the covered entity may make the requested use or disclosure;" 4) "[a] description of each purpose of the requested use or disclosure;" 5) "[a]n expiration date or an expiration event;" and 6) the signature of the individual and date signed. *Id.* at § 164.508(c). A valid authorization may need to contain additional elements. *Id.* at § 164.508(b)(1). Failure to include the necessary elements shall render the authorization invalid. *Id.* at § 164.508(b)(2).

174. *Id.* at § 164.506(c). Health care operations purposes, generally thought of not as directly advancing health care but as supporting health care treatment and payment, have certain limitations on disclosure to other health care providers, while treatment and payment purposes are virtually unrestrained. *See id.* at § 164.506(b)(4) (limiting disclosures for certain health care operations purposes). *See also id.* at § 164.522 (discussing patient optional and required restrictions on usage and disclosure of protected health information).

175. *Id.* at § 164.508(a)(2).

176. *Id.* at § 164.501.

177. HIPAA Privacy Rule, *supra* note 155, at 82514.

consent to use the information for treatment,[178] and required an authorization for all other uses and disclosures, subject to certain exceptions.[179] Likely due to comments from mental health practitioners, HHS recognized the need to provide greater protections and more stringent requirements regarding this information.

In addition to applying to covered entities, HIPAA applies to business associates.[180] Business associates generally are those entities that provide some type of service to covered entities, for which protected health information is required.[181] More specifically, a business associate "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA] . . . or provides . . . legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity."[182] Before a covered entity can provide protected health information to a business associate, the covered entity and business associate must enter into a business associate agreement.[183] The business associate can then use or disclose the information in accordance with the business associate agreement[184] but must also obtain a similar agreement with any subcontractors.[185]

Chatbots may be regulated either as covered entities or business associates under HIPAA. To be regulated as a covered entity, a chatbot would need to be considered a "health care provider" and engage in "electronic transactions."[186] Since a "health care provider" is anyone who engages in "health care" in the ordinary course of business, this broad definition would encompass these tools.[187]

---

178. *Id.*

179. *Id.* *See* 45 C.F.R. § 164.508(a)(2) (setting forth limited uses and disclosures without an authorization).

180. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, § 13401, 123 Stat. 260 (2009). Due to the broad definition of "business associate," some have criticized this application as being overly broad. *See, e.g.*, Stacey A. Tovino, *Gone Too Far: Federal Regulation of Health Care Attorneys*, 91 OREGON L. REV. 813 (2013) (arguing that attorneys should be exempted from HIPAA).

181. 45 C.F.R. § 160.103.

182. *Id.*

183. *Id.* at § 164.502(e)(2). The rule does not specify *when* the satisfactory assurance of a business associate must be obtained. *Id.* Practically speaking, however, this should occur before protected health information is disclosed.

184. *Id.* at § 164.504(e)(2).

185. *Id.* at § 164.502(e)(1)(ii).

186. *See id.* at § 160.103 (defining a covered entity).

187. *Id.*

According to online guidance for app developers created by HHS and the FTC, certain types of mobile apps may in fact be considered health care providers under HIPAA if they engage in "electronic transactions."[188] Thus, when designing its business model, these tools could focus on models that do not involve the acceptance of insurance and therefore do not engage in electronic transactions. Since chatbots engage consumers but do not bill insurance, they are health care providers but not covered entities.[189]

Since these chatbots are not covered entities,[190] they could be considered business associates. This, however, seems unlikely, even if they are working with mental health providers. Business associates must directly contract with a covered entity.[191] As a number of mental health professionals do not accept insurance, these providers would not be subject to HIPAA.[192] If an app or chatbot engaged with a covered entity, it would be considered a business associate. However, the confidentiality restrictions for the usage and disclosure of data would apply *only* for that specific covered entity.[193] Thus, if

---

188. *Mobile Health Apps Interactive Tool*, FED. TRADE COMM'N (last updated Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool [hereinafter *Mobile Tool*]. The interactive tool focuses narrowly on those mobile apps that require a prescription to access. *Id.* (discussing HIPAA applicability to those apps that require prescriptions at question 5). As of April 30, 2018, the guidance has not been updated to account for the enactment of the 21st Century Cures Act and the changes made to medical devices. *Id.* Further, this Article does not consider the potential incentive for developers to obtain FDA approval or clearance in order to be considered "health care providers" instead of "business associates." *See* 45 C.F.R. §164.103 (defining a covered entity as a "health care provider" who engages in "transactions").

189. This would be similar to those mental health professionals who are still considered health care providers but who are nonetheless not subject to HIPAA. *See* Varney, *supra* note 166.

190. Even assuming that chatbots satisfied the definition of covered entity by engaging in electronic transactions, it is unclear how the heightened protections on psychotherapy notes would apply. *See* 45 C.F.R. § 164.508(a)(2). As discussed previously, a chatbot could be considered a health care provider. *See supra* notes 185-89 and accompanying text. However, as an artificial intelligence module, it is unclear what may qualify as "psychotherapy notes" in accordance with the definition under HIPAA. *See* 45 C.F.R. § 164.501 (defining psychotherapy notes). Psychotherapy notes may be interpreted to encompass the analysis of natural language processing conducted by the app, and such an interpretation could stifle innovation in the absence of formal authorization.

191. 45 C.F.R. § 164.502(e)(2).

192. Varney, *supra* note 166.

193. The business associate in this case would be subject to all the applicable business associate requirements of HIPAA, but the use and disclosure requirements would be based on the business associate agreement. *See, e.g.*,

a chatbot does not accept insurance (or otherwise engage in electronic transactions)[194] or contract with a covered entity, it can seemingly avoid the requirements of HIPAA. Ultimately, with chatbots focusing on direct-to-consumer business models without insurance, HIPAA will not apply to them.

Though HIPAA may be the only federal general health information confidentiality law,[195] a number of states have enacted their own health information confidentiality requirements. Some are similar to, or defer to, HIPAA,[196] and others have expanded the requirements in some aspects.[197] For example, Texas has enacted specific requirements on health information similar to HIPAA as part of its Medical Records Privacy Act.[198] The Texas law also applies to covered entities and business associates, but the definition of "covered entity" is broader under Texas law.[199] The Texas law applies to anyone who "comes into possession of protected health information or obtains or stores protected health information,"[200] using HIPAA's definition of PHI.[201] Texas law provides some additional and different requirements than HIPAA, including

---

Frank Pasquale and Tara Adams Ragone, *Protecting Health Privacy in an Era of Cloud Computing*, 17 STAN. TECH. L. REV 595, 609-14 (2014).

194. *See infra* notes 195-199 and accompanying text.

195. INST. OF MED., *supra* note 153, at 405. HIPAA does provide for a limited preemption of certain state statutes. *Id.* at 407.

196. *Id.* at 409. *See, e.g.*, Va. Code. Ann. § 32.1-127.1:03 (2018) (providing for health information confidentiality and incorporating references to HIPAA).

197. *See, e.g.*, Tex. Health & Safety Code § 181 eq. seq. (2018).

198. *Id. See also* Cal. Civil Code § 56.10 (2018) (further delineating what individuals can do with information beyond the uses provided for in HIPAA).

199. Tex. Health & Safety Code § 181.001 (defining a "covered entity").

200. *Id.* at § 181.001(2). The Texas law also encompasses any person who:

> for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing or transmitting protected health information. This term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site;
>
> comes *into possession of protected health information*;
>
> *obtains or stores protected health information under this chapter*; or
>
> is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) . . . .

Id. (emphases added).

201. *Id.* at § 181.001(a) ("Unless otherwise defined in this chapter, each term that is used in this chapter has the meaning assigned by the Health Insurance Portability and Accountability Act and Privacy Standards.").

limitations on sale and disclosure.[202] However, the law still generally permits covered entities to use and disclose information for treatment and payment.[203]

The applicability and effect of the law on these chatbots, however, is minimal. As noted, those states that have adopted legislation, have done so through legislation akin to HIPAA.[204] Since chatbots are not subject to HIPAA, they will also not be subject to these state laws.[205] However, even if they were, the law may provide only limited additional protections in terms of information privacy. Using Texas law as an example, chatbots would fall under the state law definition of "covered entity."[206] Thus, chatbot providers would be unable to use protected health information for marketing purposes,[207] but the sale or disclosure of the information would be permitted "as otherwise authorized . . . by state or federal law."[208] Since the FTC Act permits a chatbot to engage in any disclosure as long as a consumer is provided notice,[209] the chatbot would be authorized by federal law to disclose this information, making the disclosure prohibitions of the Texas law inapplicable.

C. Specific Health Confidentiality Laws

In addition to general health information confidentiality laws, federal and state governments can create (and have created) specific health confidentiality laws, increasing restrictions and protections for certain types of conditions.[210] Generally, these heightened requirements have applied to "sensitive" conditions or to mental and behavioral health concerns.[211] Often, the focus of these conditions has been to offer additional protections to the patient, due to

---

202. *See* Tex. Health & Safety Code § 181.101 (providing for additional training requirements); §§ 181.151-54 (providing additional restrictions on usage and disclosure of information).

203. *Id.* at § 181.154.

204. INST. OF MED., *supra* note 153, at 409.

205. *See supra* notes 190-200 and accompanying text (determining that chatbots will not be subject to HIPAA).

206. Tex. Health & Safety Code § 181.001.

207. *Id.* at § 181.152.

208. *Id.* at § 181.153(a)(2).

209. *See supra* Section IV.A (discussing the FTCA and similar state consumer protection acts that permit any use and disclosure of information as long as a consumer has been provided notice thereof).

210. *See* Confidentiality of Substance Use Disorder Patient Records, 42 C.F.R. pt. 2 (2018); INST. OF MED., *supra* note 153, at 409-16 (discussing state mental health and substance use confidentiality requirements).

211. INST. OF MED., *supra* note 153, at 409-16.

heightened sensitivities or stigma surrounding their health conditions.[212]

At the federal level, the specific health confidentiality legislation and regulations are commonly referred to as the Confidentiality of Substance Use Disorder Patient Records.[213] Congress enacted two laws in the early 1970s regarding drug and alcohol use disorder treatment programs.[214] Each law allocated funds to assist treatment facilities with the treatment of substance use disorder and alcoholism.[215] As part of the disbursement of funds, Congress expressly required that all "[r]ecords of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any" program authorized under the respective acts be maintained as confidential subject to certain explicit exceptions.[216]

After the enactment of these laws, the Department of Health, Education, and Welfare and the Special Action Office for Drug Abuse Prevention promulgated confidentiality rules for alcohol and substance use disorder, 42 C.F.R. Part 2 ("Part 2"), in 1975.[217] Alcohol and substance use patients were considered a vulnerable population, and the goal of the confidentiality requirements was "to ensure that a patient . . . is not made more vulnerable by reason of the availability of their patient record."[218] Thus, the confidentiality requirements focus broadly on "any information which would identify a patient as having or having had a substance use disorder."[219] This broad definition would seemingly prohibit any disclosure of any information that could identify the patient.[220] Thus, any disclosure could potentially be considered impermissible.

Though the confidentiality restrictions appear broad, the applicability of this regulation to entities is actually narrow in scope.

---

212. Confidentiality of Substance Use Disorder Patient Records, 42 C.F.R. pt. 2 (2018).

213. *Id.*

214. Federal Assistance for State and Local Alcoholism and Alcohol Abuse Programs Act, Pub. L. No. 93-282, 88 Stat. 125 (May 14, 1974); Drug Abuse Office and Treatment Act of 1972, Pub. L. No. 92-255, 86 Stat. 66 (Mar. 21, 1972).

215. 88 Stat. 127-28; 86 Stat. 71.

216. 88 Stat. 131; 86 Stat. 79.

217. Confidentiality of Alcohol and Drug Abuse Patient Records, 40 Fed. Reg. 27802 (finalized July 1, 1975).

218. 42 C.F.R. § 2.2(b)(2) (2018).

219. *Id.* at § 2.12(e)(3).

220. *Id.* at § 2.12(e)(3). *See also id.* at § 2.12(e)(1) ("These regulations cover any information (including information on referral and intake) about patients receiving diagnosis, treatment, or referral for treatment for a substance use disorder created by a part 2 program.").

The substance and alcohol use disorder regulations only apply to federally assisted programs.[221] The regulations do not define a "federally-assisted program,"[222] but instead separately define a "program" and what it means to be "federally-assisted.".[223] The regulations define a program as "an individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment."[224] Furthermore, the regulations define "federally-assisted" to include programs:

> [C]arried out under a license, certification, registration, or other authorization granted by any department or agency of the United States including but not limited to:
>
> Participating provider in the Medicare program;
>
> Authorization to conduct maintenance treatment or withdrawal management; or
>
> Registration to dispense a substance under the Controlled Substances Act, to the extent the controlled substance is used in the treatment of substance use disorders . . . .[225]

---

221. *Id.* at §§ 2.11-2.12.

222. While the regulations do not provide a definition of a "federally assisted program," the definitions define a "Part 2 program" as a "federally assisted program." *Id.* at § 2.11.

223. *Id.* The definition of "federally assisted" under § 2.11 refers to § 2.12(b). *Id.*

224. *Id.* There are two other components within the definition of a program:

> (2) An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
>
> (3) Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.

Id.

225. *Id.* at § 2.12(b). A federally assisted program may also be "conducted in whole or in part . . . by any department or agency of the United States," subject to certain exceptions. *Id.* at § 2.12(b)(1). It may also be "a recipient of federal financial assistance in any form . . . or [c]onducted by a state or local government unit which . . . receives federal funds which could be spent for [a] substance use disorder program." *Id.* at § 2.12(b)(3). Finally, a federally assisted program may be tax-exempt or may permit for contributions to be tax-deductible. *Id.* at § 2.12(b)(4).

In contrast to the narrow definition of program, the definition of "federally-assisted" indicates that *any* approval from *any* agency used to support treatment of substance use disorder would suffice to impose the confidentiality requirements.[226]

Part 2 is not absolute in its prohibition on disclosure. First, Part 2 permits disclosure with patient consent.[227] However, a patient consent under Part 2 is more analogous to a patient authorization under HIPAA than consent.[228] Furthermore, upon disclosure, the disclosing entity must provide the receiving entity with a statement that the information cannot be re-disclosed.[229] Second, Part 2 permits disclosure to a qualified service organization "(QSO"), which is an entity that provides services to a federally assisted program and has a contract acknowledging the limitations in disclosure under Part 2.[230] Functionally, a QSO is akin to a business

---

226. *Id.* at § 2.12(b)(2). Even though there are potential exceptions to this broad definition, *id.* at § 2.12(c), federal-assistance requires any "authorization granted by *any* department or agency." *Id.* at § 2.12(b)(2).

227. 42 C.F.R. § 2.31. Recognizing the advent of healthcare information technology programs, such as health information exchanges ("HIEs"), SAMHSA recently updated its rule to account for uses and disclosures by HIEs and other health care providers. Confidentiality of Substance Use Disorder Patient Records, 82 Fed. Reg. 6052 (finalized Jan. 18, 2017).

228. *Compare* 42 C.F.R. § 2.31 (setting forth the requirements of a consent under SAMHSA) *with* 45 C.F.R. § 164.508(c) (2018) (setting forth the requirements of HIPAA authorization) *and supra* Section IV.A. For patient consent to be valid under SAMHSA, it must include:

> The name of the patient.
>
> The specific name(s) or general designation(s) of the part 2 program(s), entity(ies), or individual(s) permitted to make the disclosure.
>
> How much and what kind of information is to be disclosed, including an explicit description of the substance use disorder information that may be disclosed.
>
> (i) The name(s) of the individual(s) to whom a disclosure is to be made; . . .
>
> The purpose of the disclosure. . . .
>
> A statement that the consent is subject to revocation at any time except to the extent that the part 2 program or other lawful holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it. . . .
>
> The date, event, or condition upon which the consent will expire if not revoked before. . . .
>
> The signature of the patient . . .
>
> The date on which the consent is signed.

42 C.F.R. § 2.31(a).

229. *Id.* at § 2.32(a).

230. *Id.* at § 2.11.

associate under HIPAA.[231] Third, Part 2 permits disclosures in specific circumstances, such as medical emergencies,[232] research,[233] and audits and evaluations,[234] but requires a court order for other disclosures.[235] Thus, there are instances in which the information can be used and disclosed; however, there is still recognition of a vulnerable patient population and the need to protect sensitive information from unnecessary disclosure.

The requirements of Part 2 do not apply to the specific chatbots discussed in this Article; however, that does not mean that they will never apply to chatbots. Though SAMHSA has likely not considered this issue, the breadth of the definition of "federally-assisted" would likely encompass FDA approval or clearance.[236] Thus, a chatbot or technology that required FDA approval and specifically focused on substance use technologies would likely come within the purview of Part 2.

As an example of a similar technology subject to this regulatory regime, the FDA recently approved a mobile medical app for the treatment of substance use disorders.[237] Though it was not a chatbot, it did receive FDA clearance.[238] The app also specifically held itself out for the treatment of substance use disorders, indicating it would be subject to Part 2.[239] At the moment, no chatbot app is within the purview of Part 2, but this example reinforces the applicability.[240]

---

231. *Compare* 45 C.F.R. § 160.103 (defining a business associate) *with* 42 C.F.R. § 2.11 (defining qualified service organization). *Compare* 45 C.F.R. § 164.504(e)(2) (setting forth the contractual requirements for business associates) *with* 42 C.F.R. § 2.11 (setting forth the contractual requirements with qualified service organizations).

232. 42 C.F.R. § 2.51.

233. *Id.* at § 2.52.

234. *Id.* at § 2.53.

235. *Id.* at § 2.61.

236. *See id.* at § 2.12 (providing for any approval by any agency to constitute "federal assistance"). For a discussion of different FDA approval and clearance mechanisms, see Roth, *supra* note 70.

237. *FDA Permits marketing of mobile medical application for substance use disorder*, U.S. FOOD & DRUG ADMIN. (Sept. 14, 2017), https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm576087.htm.

238. *Id.* The specific route to market encompassed the de novo review process, as it was a new technology without a substantially equivalent product currently on the market. *Id.*

239. *See* 42 C.F.R. § 2.11 (defining a program). In addition to being subject to the SAMHSA regulations, this app requires a prescription for individuals to access, indicating it is a health care provider and may be subject to HIPAA. *Mobile Tool*, *supra* note 188.

240. SAMHSA has not commented on the applicability.

States have also created heightened laws to protect substance use disorder disclosure, as well as the disclosure of mental health information, behavioral health information, and certain types of diseases.[241] All fifty states have adopted some type of mental health confidentiality restrictions, either pursuant to applicable statutes or as part of a Department of Health regulatory structure.[242] The Illinois and District of Columbia ("D.C.") statutes are illustrative.[243]

Illinois provides a heightened degree of protection to any communications made "to a therapist or to or in the presence of other persons during or in connection with providing mental health or developmental disability services to a recipient."[244] The Illinois statute encompasses all "records and communications *regardless* of whether the records and communications are made or created in the course of a therapeutic relationship."[245] However, it does provide certain narrow instances in which information can be disclosed.[246]

The D.C. statute goes one step further than the Illinois statute by encompassing data collectors as well.[247] The statute prohibits the use or disclosure of mental health information by mental health professionals, mental health facilities, and data collectors.[248] It defines a data collector as "a person . . . who regularly engages, in whole or in part, in the practice of assembling or evaluating client mental health information."[249] However, the definition of mental health information only encompasses "mental health professionals," a class that is limited to specifically enumerated licensed

241. NAT'L ASS'N OF STATE MENTAL HEALTH PROGRAM DIRECTORS, 2016 COMPILATION OF STATE BEHAVIORAL HEALTH PATIENT TREATMENT PRIVACY AND DISCLOSURE LAWS AND REGULATIONS (Sept. 2016), https://www.nasmhpd.org/sites/default/files/Assessment%209_2016%20Compilation%20of%20State%20Behavioral%20Health%20Patient%20Treatment%20Privacy%20and%20Disclosure%20Laws%20and%20Regulations%20-%209-2016_1.pdf [hereinafter 2016 COMPILATION] (identifying state laws and showcasing the applicability to mental health professionals).

242. *Id. See also* Jaffee v. Redmond, 518 U.S. 1 (1996) (noting that all fifty states have adopted some type of mental health privilege).

243. Illinois Mental Health and Developmental Disabilities Confidentiality Act, 740 Ill. Comp. Stat. § 110/2 (2018); D.C. Code § 7-1201.02 (2018).

244. Illinois Mental Health and Developmental Disabilities Confidentiality Act, 740 Ill. Comp. Stat. § 110/2 (2018).

245. *Id.* at § 110/3.

246. *Id.* at § 110/6-12.2. *See also id.* at § 110/5 (noting that disclosure must occur to a specific individual as discussed in the statute, with patient consent, or in accordance with a specific statutory exception).

247. D.C. Code § 7-1201.02 (2018).

248. *Id.*

249. *Id.* at § 7-1201.01.

professionals.[250] Therefore, though organizations that regularly assemble or evaluate mental health information may be subject to confidentiality obligations, the obligations apply only to information received from a traditional, licensed mental health professional.[251]

While states recognize the need for heightened protections for mental health professionals and therapy, the main focus is on those individuals licensed by the state as mental health providers.[252] Chatbots or mobile apps are not included in these apps, unlike Part 2 which includes them due to its broad scope.[253] Furthermore, although the D.C. statute imparts data confidentiality requirements on data collectors,[254] the information protected ultimately must first be obtained by a mental health professional.[255] While chatbots or software-based therapy may obtain similar information to that obtained by mental health professionals, since direct initial involvement of a mental health profession, information is not subject to the state protections. Thus, there are no requirements on chatbots or similar apps to maintain confidentiality.

V. MINDING THE CONFIDENTIALITY GAP

Part IV highlights a gap in the existing privacy framework in the United States's non-traditional mental health providers, new and emerging apps are not subject to the complicated regulatory framework without affording users protection against further disclosure. Some scholars have focused on tele-psychiatry and tele-mental health confidentiality concerns,[256] and others have discussed the safety and efficacy of these new technologies.[257] This Article uses somewhat of a hybrid approach, arguing that these chatbots function similar to traditional mental health providers and should be afforded confidentiality protections, even if not subject to FDA oversight.

250. *Id.*

251. *Id.*

252. *See* 2016 COMPILATION, *supra* note 241.

253. As shown in notes 226-246 and accompanying text, the broad definitions seemingly encompass chatbots or mobile medical apps, even though the focus was on substance use and mental health professionals. *See supra* notes 231-250 and accompanying text.

254. D.C. Code § 7-1201.02.

255. *Id.* at § 7-1201.01.

256. Winnike & Dale III, *supra* note 6, at 92-94.

257. Lee, *supra* note 65.

A. Arguments for Heightened Protections

Before addressing the need for these protections, it is helpful to understand the Supreme Court's guideposts in considering whether and when to provide strong confidentiality protections through creation of a federal privilege.[258] In *Jaffee v. Redmond*, the Supreme Court considered the nature of the therapeutic relationship,[259] the existence of other laws providing a privilege,[260] and issues related to access and cost,[261] in order to justify the creation of psychotherapist-patient and social worker-patient privileges.[262] The Court believed that the nature of the relationship required the parties "to communicate freely without the fear of public disclosure." [263] The Court looked to existing state laws providing privilege and noted that all 50 states have adopted some form of the . . . privilege."[264] The Court further considered the practical considerations of cost and access, and ultimately decided to extend the psychotherapist privilege to encompass licensed clinical social workers.[265] Applying these previously enunciated concepts and principles indicates the need for mental health confidentiality regulations for apps, as these apps use similar techniques and provide similar support as these professionals.

1. Nature of the Therapeutic Relationship

Mental health professionals view confidentiality as paramount to their profession given the more intimate disclosures that occur compared to those of healthcare providers treating the body.[266] Unlike physical ailments, mental health conditions may be less obvious.[267] Oftentimes, when someone has a physical ailment, it can

---

258. Jaffee v. Redmond, 518 U.S. 1, 3 (1996). This Article focuses solely on the question of whether confidentiality requirements are necessary and does not contemplate the question of whether the additional protections of a privilege apply. For an evaluation of privilege and confidentiality statutes, see Steven R. Smith, *Medical and Psychotherapy Privileges and Confidentiality: On Giving with One Hand Removing with the Other,* 75 KY. L.J. 473 (1986).

259. *Jaffee*, 518 U.S. at 10-12.

260. *Id.* at 12-15.

261. *Id.* at 15-17.

262. *Id.* at 18.

263. *Id.* at 6 (citing Jaffee v. Redmond, 51 F.3d 1346, 1355-56 (7th Cir. 1995)). The Court added, "the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment." *Id.* at 10.

264. *Id.* at 12.

265. *Id.* at 16-17.

266. Winsdale & Ross, *supra* note 7.

267. Winsdale & Ross, *supra* note 7, at 622.

be readily apparent or easily seen.[268] With a mental ailment, by contrast, nothing is known about the condition or the patient's thoughts or feelings unless it is disclosed.[269] No one knows the inner workings of another person's mind unless and until that individual chooses to be afforded the benefit of treatment and to give up their privacy right to that information.[270] This requires ultimate confidentiality between provider and patient, which "is necessary to develop the trust and confidence important for therapeutic intervention."[271]

Apps involving chatbots, app developers, and other similar entities seek to create or simulate an intimate relationship or similar relationship to that created by mental health professionals.[272] App developers want individuals to use their product and they want individuals to think they are having an interaction with a trusted resource.[273] In fact, user responses indicate that users are creating relationships with apps which involves a degree of intimacy and trust.[274] Confidence and trust are the cornerstones of the mental health treatment relationship,[275] and apps are laying them, encouraging individuals to disclose how they feel in exchange for feeling better—exactly like psychotherapy.

2. Extent of Existing Laws

Existing laws do not currently protect mental health information shared with apps, because these tools are not currently thought of as mental health providers. Healthcare confidentiality laws focus predominantly on *people*—such as physicians, or entities, such as

---

268. *Id.* ("The patient who goes to his physician with fevers, lumps, rashes, or pains does not construe the relationship to be one in which he may *choose* to reveal or not reveal such information as he has about his physician condition or compliant . . . .").

269. *Id.* at 620.

270. *Id.* ("Others are prepared to sit with a patient for an indefinite period with no words exchanged on the assumption that the patient's sense of what and when private information needs to be revealed must be respected, not only because it demonstrates respect for the person's autonomy, but also because respecting the patient's decision not to reveal any personal information may itself be therapeutic.")

271. 55 Pa. Code. § 5100.31(b). It also states, however, that "full confidentiality cannot be guaranteed to everyone as a result of Federal and State statutes, which require disclosure of information for specific purposes . . . ." *Id.*

272. Hoffer, *supra* note 46; Fitzpatrick et al., *supra* note 54; Wallach, *supra* note 59.

273. *See supra* text accompanying note 272.

274. Fitzpatrick et al., *supra* note 54.

275. Winsdale & Ross, *supra* note 7, at 622.

hospitals—as being in the business of providing health care.[276] This is most pronounced in the area of mental health, as the existing laws in all states focus on mental health providers as individuals and only encompass technologies in a very specific, limited circumstance.[277] The existing legal framework has not kept pace with the advancement of new technologies, which challenge the very notion of who can provide healthcare. It is only through happenstance and broad drafting that certain technologies are encompassed by the existing framework.[278] It is time to update the law to accommodate new technologies and modes of therapy.

While the laws may not have kept apace of new technologies, professional organizations, such as the American Psychiatric Association and American Psychological Association are aware of and have raised concerns about these emerging mental health technologies. At the release of Woebot, John Torous, the Chair of the American Psychiatric Association's Smartphone App Evaluation Work Group, raised concerns about the need to maintain the confidentiality of information.[279] Torous also raised concerns about the effectiveness of these apps, but noted they have the ability to transform mental health services by providing support to people when they need it as opposed to waiting for an appointment.[280] The American Psychiatric Association ("APA") has adopted a rating system and an evaluation rubric for its members in determining when and whether to recommend apps for patients.[281] This is geared towards individuals currently under the direction of a mental health professional, using apps recommended by the mental health professional.[282] However, the APA suggests its members ask questions that the app developers themselves[283] may be unable to

276. *See* 2016 COMPILATION, *supra* note 241 (identifying state laws and showcasing the applicability to mental health professionals).

277. *Id. See also supra* Section IV.C (identifying limited scenarios in which these laws encompass technology).

278. *See supra* Section IV.B (noting that apps constitute "health care providers" under HIPAA), IV.C (noting that apps constitute "federally-assisted programs" under SAMHSA).

279. Nutt, *supra* note 65.

280. *Id.*

281. *App Evaluation Model*, AM. PSYCHIATRIC ASS'N, https://www.psychiatry.org/psychiatrists/practice/mental-health-apps/app-evaluation-model (last visited Apr. 30, 2018).

282. *Id.* at Step 2.

283. A prescription mobile medical application, Welldoc, has adopted a health information privacy note, which does not affirmatively state that Welldoc is subject to HIPAA. *Privacy Policy*, WELLDOC, https://www.bluestardiabetes.com/

determine, such as whether an app needs to be HIPAA-compliant.[284] Standardizing confidentiality requirements instead of deferring to the existing FTC Act can assist and reassure psychiatrists and users in the recommendation and adoption of apps.

Similarly, the American Psychological Association ("Association") considered the benefit of Woebot and other "Just-In-Time Adaptive Interventions" to combat negative and unhealthy behaviors when the risk of harm to the patient is higher, instead of at a later time.[285] However, the Association seems skeptical of new therapy modalities due to potential legal and ethical issues.[286] The Associate Executive Director for Practice Research and Policy at the Association believes that technology innovators may not fully understand issues related to HIPAA, licensing laws, and confidentiality.[287] While her comments speak predominantly to telepsychiatry services in which clinicians are involved,[288] there may be greater concerns when those same technologists do not engage clinicians and rely solely on their ability to program artificial intelligence. That is not to say that the standards should be different if a clinician is engaged in the creation of apps. Rather, the differences in understanding should be aided by a level playing field: clear, applicable confidentiality requirements for chatbots and apps to follow.

3. Stigma, Access, and Cost

Another set of factors to consider in determining whether to extend confidentiality protections is that of stigma, access, and cost. App users may be concerned about stigma or negative associations or connotations. As one author has put it, "[a] fundamental assumption of psychoanalysis is that patients have feelings, beliefs, and desires that are so shameful and embarrassing or painful to the patient that he represses them and is unable to consciously

---

Portal/Guest/PrivacyPolicy.htm (last visited Apr. 30, 2018). This could potentially be considered deceptive as it is unclear.

284. *App Evaluation Model*, *supra* note 281. The evaluation rubric also suggests asking "What data are collected?" and "Who are data shared with/What data are shared?" *Id.*

285. Amy Novotney, *Trends report: Technology is revolutionizing practice*, MONITOR ON PSYCHOL., Nov. 2017, at 78, http://www.apa.org/monitor/2017/11/trends-technology.aspx [hereinafter *Revolutionizing Practice*].

286. *See generally* Amy Novotney, *A growing wave of online therapy*, MONITOR ON PSYCHOL., Feb. 2017, at 48, http://www.apa.org/monitor/2017/02/online-therapy.aspx [hereinafter *Growing Therapy*].

287. *See id.* at 51.

288. *Id.*

formulate, much less acknowledge them, as his own."[289] While this may largely be applicable to more advanced conditions, the same could be said of more minor conditions: individuals may avoid seeking treatment because they feel ashamed of even mildly negative feelings or are too embarrassed to disclose their feelings or beliefs to another person.[290] Individuals may feel more comfortable discussing these thoughts and beliefs with a machine-operated app due to a lower perception of judgment.[291] These same individuals may assume a degree of confidentiality,[292] or may feel that the lack of adequate confidentiality protections is "unfair or deceptive," given the nature of the service.[293] Assurances of confidentiality, in this case through regulation, can help to further uses and disclosures.[294]

In fact, the adoption of these technologies and protections may operate to increase access and reduce the stigmatization of mental health concerns.[295] Access to mental health professionals has had somewhat of an interesting history, with Congress focusing on access through payment equity by healthcare plans.[296] However, instead of embracing health plans and insurance companies, a number of mental health professionals have simply engaged in out of pocket or cash-pay practices.[297] Thus, cost and access may operate to prevent

---

289. Winsdale & Ross, *supra* note 7, at 641.

290. *Id. See also* Patrick Corrigan, *How Stigma Interferes with Mental Health Care*, 59 AM. PSYCHOLOGIST 614, 615-16 (2004).

291. Kristen C. French, *Your New Best Friend: AI Chatbot*, FUTURISM (Jan. 29, 2018), https://futurism.com/ai-chatbot-meaningful-conversation.

292. This assumption would be based on the fact that mental health professionals offer confidentiality, and that since consumers are seeking a similar service, similar regulations would apply.

293. Individuals may believe it is implicitly deceptive to offer this service, but not provide the same degree of confidentiality. *See* Gregory Klass, *Meaning, Purpose, and Cause in the Law of Deception*, 100 GEO. L.J. 449, 486-87 (2012) (discussing implicitly deceptive false advertising claims).

294. Individuals may not be able to obtain complete confidentiality, *see* 55 Pa. Code. § 5100.31(b) ("full confidentiality cannot be guaranteed to everyone as a result of Federal and State statutes, which require disclosure of information for specific purposes . . . ."), but regulations can aid in attempting to provide some degree of confidentiality to an area of information traditionally afforded confidentiality protections.

295. *Revolutionizing Practice*, *supra* note 285.

296. *See, e.g.*, Mental Health Parity and Addiction Equity Act of 2008, Pub. L. No. 110-343, §512 (2008).

297. Demobsky, *supra* note 166 (noting that mental health professionals tend to gravitate towards cash payment, with the majority of services going to the wealthy); Varney, *supra* note 166. As discussed previously, the avoidance of insurance also results in an avoidance of being subject to HIPAA, likely incentivizing mental health professionals to avoid billing insurance.

an individual from obtaining needed mental health services. First, the consumer must determine whether their health insurance covers such a plan or whether they would need to pay out of pocket. The cost alone of seeking mental health counseling, may create a potential burden prohibiting access.[298] Second, assuming a plan covers mental health services, the consumer would need to identify a provider of mental health services and schedule an appointment. Similar to seeing physicians, there may be a wait list for access: appointments may not be for a few weeks out.[299] While some mental health professionals may have "emergency" time-slots for individuals that need more urgent care, [300] it seems likely that there will be a lag time between a mental health issue and access to care. For example, an individual may undergo a panic attack on a Thursday afternoon. They may be fortunate enough to access an employee assistance program ("EAP") through their employer, which provides a certain number of counseling sessions. They may call a counselor on Thursday evening or Friday morning who is unable to respond until the following Monday. Then, it may take an additional week or two to finally obtain access to mental health services. Though certain tele-health services may be able to increase access and maintain confidentiality concerns through a direct-to-consumer model,[301] similar scheduling issues may remain. Chatbots, and similar technologies, provide individuals more of an on-demand access to these services to respond to mental health challenges, instead of incurring delays.[302]

This increased access may combat the stigmatization of mental health issues. As discussed previously, certain laws were passed in order to protect patients in light of prevailing social stigma concerns.[303] Mental health problems continue to be stigmatized in our society.[304] In fact, one scholar shows the degree of stigma

298. Demobsky, *supra* note 166.

299. *See, e.g.*, *'Concern' as mental health wait times double in six years*, BBCNEWS (July 25, 2017), http://www.bbc.com/news/uk-wales-40716616. This is a bit of an extreme case as it deals with the U.K.; however, minimal information is available for the U.S. outside of the inpatient or emergency setting.

300. *See Tired of the Wait: ER Doctors Make the Case for Mental Health Reform*, NATIONAL ALLIANCE OF MENTAL ILLNESS (Oct. 25, 2016), https://www.nami.org/About-NAMI/NAMI-News/2016/Tired-of-the-Wait.

301. *Id. See also* Josh Sherman, *Double Secret Protection: Bridging Federal and State Law to Protect Privacy Rights for Telemental and Mobile Health Users*, 67 Duke L.J. 1115, 1136-1146 (2018) (discussing telemental compliance concerns).

302. *Growing Therapy*, *supra* note 286; *Revolutionizing Practice*, *supra* note 285.

303. *See, e.g.*, 42 C.F.R. pt 2 (2018).

304. Corrigan, *supra* note 290.

associated with mental health issues may prevent individuals from seeking treatment.[305] Furthermore, stigma can prevent individuals from obtaining employment or housing due to mental health-related concerns by the renter or employer.[306] In addition to this public stigmatization, individuals may have their own views on people with mental illness or on treatment thereof that prevent them from seeking treatment.[307]The creation of confidentiality requirements for apps may help curb these stigmas—both through increasing utilization of mental health services and through recognizing that individuals may seek support with their mental health without being "labeled" or "stigmatized" for suffering from a mental illness.[308] Further, the current lack of protection continues to perpetuate the stigma of mental illness and prohibit or prevent individuals from accessing treatment.

Examples may assist in highlighting exactly how the lack of confidentiality requirements could exacerbate existing mental health issues and further stigmatize individuals. Consider one individual who has recently faced a traumatic life event. The individual exhibits signs of anxiety and depression, which are perfectly normal considering the disturbing event. Prior to seeking support from an app, the individual has been prone to eating ice cream and watching Netflix. He then thinks to try the app, as he is concerned about being judged by a therapist. In talking to the app about feelings, he mentions his increased ice cream and Netflix consumption. Two weeks later, he begins to receive marketing and additional promotions for Hulu, Amazon Prime, HBO Go, YouTube Red, Fandango, and movies, as well as marketing and promotions for local restaurants. His mental state does not improve. He not only continues to feel anxious and depressed, he now notices weight gain and is experiencing increased feelings of self-loathing. However, that further prevents him from seeking therapy. Under existing laws, this chain of events is fully legal.

In a more troubling example, an individual suffers from stress and anxiety at work, as well as some minor paranoia. He believes this is temporary, having never had symptoms before. Due to his high-demand work, he does not believe he can take time off to see a therapist and he is concerned about being deemed unable to handle his workload. He learns about these new technologies and decides to give them a try. He tells the chatbot that he has been

305. *Id.* at 615-6.
306. *Id.* at 616.
307. *Id.* at 617-18.
308. *Cf. id.* at 618.

thinking about going to therapy, going for vacations, and drinking alcohol. He begins to receive new advertisements for mental health professionals, for vacations, and for alcohol. His feelings of anxiety and paranoia increase until he decides to take his own life. While this may be an extreme case—and may have required the app to alert the individual of the need for professional help[309]—it assists in showcasing the potential dangers of unregulated confidentiality in this area. These considerations are the same as presented previously in this article, in advocating for the need for confidentiality legislation to protect information shared through chatbots and apps.

4. Review of *Jaffee* Factors

In *Jaffee*, the Supreme Court considered the nature of the therapeutic relationship, [310] the existence of other laws providing a privilege, [311] and issues related to access and cost,[312] to justify extending a privilege. [313] As discussed above, chatbots and other apps provide therapy-like settings, for which confidentiality is paramount. While states recognize the need for confidentiality requirements for "traditional" mental health providers, chatbots and apps, which challenge traditional notions of healthcare providers, are not covered by those statutes while they should be. The technology has progressed to the stage where it can provide adjunctive support similar to that provided by mental health professionals—if not potentially changing the way mental health practitioners practice—and the law must adapt. Furthermore, these types of technologies can assist in decreasing stigma and increasing access to mental health treatment, and they can provide access to therapy to those who previously could not afford it. Thus, a review of these factors indicates that information collected by mental health chatbots and other similar apps should be recognized as confidential by appropriate legislation.

---

309. Though outside the scope of this work, it is interesting to consider to what extent these types of apps may have duties that are typical for mental health professionals. For example, in what instances and how may a chatbot have a duty or obligation to refer an individual to treatment? Similarly, when and how may these technologies have a duty to warn? And finally, although this Article focuses solely on the question of confidentiality, it is interesting to consider how such information could be introduced to show an individual's mental state at trial, as well as whether a potential privilege may apply to this information.

310. *Jaffee*, 518 U.S. at 10-12 (1996).

311. *Id.* at 12-15.

312. *Id.* at 15-17.

313. *Id.* at 18.

B. Arguments Against Heightened Protections

While this Article advocates for additional protections on these software-therapy apps, it will consider arguments posed by opponents of such legislation. First, opponents argue that while the information is mental health-related, the context is not sensitive enough to require additional protections. Second, opponents argue that these nascent applications of the technology are still in their infancy and that legislation would damage innovation. Finally, opponents believe that if developers seek to provide additional protections for their users, users will choose those apps, and the free-market will determine the winners and losers. None of these arguments is particularly convincing and will be dealt with in turn.

1. Context Does Not Require Additional Protections

The first argument—that there is nothing special about the context or content to require additional protections—seems akin to the dissent's argument in *Jaffee*. In Justice Scalia's dissent, he takes issue with the expansion of psychotherapist-patient privilege to encompass licensed social workers and therapists.[314] For Scalia, the issue rested on the differing licensure and training requirements, leading him to argue that social workers did not have the necessary professional experience and training to afford them a privilege.[315] Further bolstering his position, he noted that the law has not traditionally afforded a privilege to a plethora of people who can assist with an individual's mental health: "parents, siblings, best friends and bartenders—none of whom was awarded a privilege."[316] Thus, he argued that without certain minimal licensing, training, or testing requirements, no confidentiality should be afforded.

Evaluating Scalia's position and arguments in this context leads to the proposition that only apps that have been received FDA approval or clearance should be subject to confidentiality requirements.[317] While the type or scope of FDA clinical trials for this technology is unclear,[318] trials would focus on safety and efficacy, ensuring the technology had met sufficient training

---

314. Jaffee v. Redmond, 518 U.S. 1, 21 (1996) (Scalia, J., dissenting).

315. *Id.* at 29-30.

316. *Id.* at 22.

317. The analogy in this case would be that a psychotherapist or social worker is akin to an approved or cleared app, while non-FDA-approved apps would be more akin to family members. For a discussion of FDA approval and clearance, see Roth, *supra* note 70, at 373-381.

318. Lee, *supra* note 65, at 95-96.

requirements to treat an individual's mental health.[319] However, the potential lag time in the development of this process runs up against some of the practical realities of the use and growth of this technology, as well as the current state of the regulatory FDA oversight.[320] As the FDA evaluates its oversight and approval process, the FDA may begin to mandate confidentiality as part of the "safety" of the app. At the current time, though, these types of apps appear to not be subject to FDA approval, and the costly approval process would disincentivize app developers from seeking clearance or approval.[321] Furthermore, with the growth of other chatbot technologies including Alexa, Siri, and Google Home,[322] it appears to only be a matter of time before users start asking these technologies to help them feel better or to play a certain type of music to make them happy.[323] That is still the case even if these apps are not trained in CBT or otherwise intended to be used for chat or support.[324] This seems to further advocate the need for independent confidentiality regulations.[325]

---

319. *Id.* at 91.

320. *Id.* at 70-71 (discussing potential risks as this technology continues to grow); *id.* at 76 ("Without the intervention of the federal government, it seems unlikely that digital psychiatric therapy developers will conduct clinical trials to ensure the safety and effectiveness of their products.").

321. *Id.* at 76. Once one device has undergone pre-market approval, other manufacturers can attempt to rely on the approval to claim "substantial equivalence," making them subject only to pre-market notification under the 510(k) process. *See* Roth, *supra* note 70, at 374-75. The FDA can always change the classification depending on the risk to require pre-market approval. *Id.* at 375.

322. Shum et al., *supra* note 2, at 3 (discussing the rise of personal assistants).

323. *See Cheer Me Up by Purposeful Life*, AMAZON.COM, https://www.amazon.com/Purposeful-Life-Cheer-Me-Up/dp/B07218DX29 (last accessed May 1, 2018). There are a number of skills that allow Alexa to provide "self-improvement" or "motivational quotes." *Alexa Skills: LifeStyle: Self Improvement*, AMAZON.COM, https://www.amazon.com/b/ref=dp_bc_3/147-4286784-6806369?ie=UTF8&node=14284843011 (last accessed May 1, 2018).

324. Though Amazon may not pursue this at the moment, Amazon's continued pursuit of health care tools may make this a viable business opportunity in the future so that the company may learn more about its users. *See* Christina Farr, *As Amazon moves into health care, here's what we know – and what we suspect – about its plans,* CNBC, https://www.cnbc.com/2018/03/27/amazons-moves-into-health-what-we-know.html (Mar. 27, 2018).

325. Another potential distinction to evaluate is the motive or interest of the individual. The mental health professional, like the app developer, has a financial interest in obtaining the information or working through the patient/user's issues. Arguably though, the app developer has a stronger financial interest than the mental health professional, as the developer can, through the use of technology, aggregate and store the information, and create secondary data streams from the information as third-party data.

Scalia's argument can be viewed in a different light: alternatively stated, the focus should not be on FDA oversight *per se*, but on oversight of the creation and marketing of the technology. With a sufficient knack for computer programming and access to information about CBT, someone can theoretically create an app and determine how to train it using cognitive behavioral techniques.[326] At the other end of the spectrum would be a group of psychotherapists working with developers and reviewing the outputs, potentially undergoing clinical trials.[327] This framework creates four different potential scenarios as set forth in the table below:

Clinician involvement, not created for mental health	Clinican involvement, created for mental health
No clinician, not created for mental health	No clinician, created for mental health

The first quadrant—clinician involvement, created for mental health—encompasses apps that are already on the market,[328] and encompasses apps that are subject to FDA approval or clearance.[329] The fourth quadrant—no clinician, created for mental health—is the primary focus of this article. The other two quadrants are outside of the scope of this Article but can be addressed briefly.

The third quadrant—no clinician, not created for mental health—is already occurring. Technologies that likely do not involve mental health clinicians and are not created for mental health include Siri, Alexa, and others.[330] These types of apps mimic the experience of talking to a friend or acquaintance, insofar as there is no expectation

326. *See* Wallach, *supra* note 59. None of the founders of Wysa have backgrounds in mental health or are clinicians. *Id.*

327. *See* Fitzpatrick et al., *supra* note 54. Woebot underwent formal clinical trials before being offered commercially. *Id.*

328. *Id.*

329. Lee, *supra* note 65, at 80 (noting the FDA need for clinical studies in certain instances).

330. Shum et al., *supra* note 2, at 3.

of confidentiality and the user has no training in mental health. These technologies may need confidentiality for other reasons,[331] but not due to their intended use and functionality. Similarly, the second quadrant—clinician involvement, not created for mental health—is occurring through technologies such as Twitter and Facebook. These apps are not designed for mental health purposes, but have clinicians attempting to determine if there are mental health connections. These apps may need confidentiality for other reasons, but not due to their use within mental health (potentially within physical or other).

The fourth quadrant is occurring, and raising significant ethical and regulatory questions.[332] This area, known as digital phenotyping, has seen social media sites use information gathered from users, in a non-clinical or non-mental health setting, in an attempt to identify correlations to mental health.[333] The ethical questions of whether and how to deal with any identification must be dealt with before identifying how to handle confidentiality.[334] Further, by comparison, these technologies are even more nascent and must be given more time to determine whether and how to operate before regulating.[335]

2. Legislation Would Damage Innovation

The second argument presented by Scalia's reasoning—that the introduction of regulation would stifle technological development—is not persuasive. While scholars have argued that "a poorly integrated patchwork of regulations could impede innovations,"[336] that is not the case with the confidentiality regulations advocated for

---

331. *See* Brad Stone, *Is Alexa Really Eavesdropping on You?*, BLOOMBERG TECH. (Dec. 11, 2017), https://www.bloomberg.com/news/articles/2017-12-11/is-alexa-really-eavesdropping-on-you-jb25c6vc (discussing privacy and confidentiality concerns raised by Alexa and the use of Alexa for a criminal prosecution).

332. Natasha Singer, *How Companies Scour our Digital Lives for Clues to Our Health*, N.Y. TIMES (Feb. 25, 2018), https://www.nytimes.com/2018/02/25/technology/smartphones-mental-health.html.

333. *Id.*

334. *Id.*

335. *Id. See also* Natasha Singer, *Risks in Using Social Media to Spot Signs of Mental Distress*, N.Y. TIMES, Dec. 26, 2014, https://www.nytimes.com/2014/12/27/technology/risks-in-using-social-posts-to-spot-signs-of-distress.html.

336. Daniel Gilman & James Cooper, *There Is a Time to Keep Silent and a Time to Speak, the Hard Part is Knowing Which Is Which: Striking a Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. TECH. L. REV. 279, 285 (2010).

in this Article. As noted in Part IV, there already exists a poorly integrated patchwork of regulations on maintaining confidentiality by mental health and mental health apps. The proposal presented here seeks to provide some consistency to the patchwork of regulations, by creating limitations on disclosure for this specific use of technology. The proposal is intended to be narrowly tailored, to a specific area where the context requires additional protections.[337] While there may be limits to the advancement of chatbot and mental health apps, the basic technology has existed for almost 50 years and is being applied in new and unique ways.[338] Further, companies may consider information obtained from users, to be part of their trade secrets—that is, the algorithms powering their artificial intelligence—and seek to maintain the confidentiality of the information to maintain competitive business advantage.[339] Therefore, the proposal presented herein would not stifle the advancement of technology, but would be in line with the concerns of business owners and entrepreneurs.[340]

3. Free-Market Argument

The final argument—suggesting that users will choose the best product—seems to encompass a few different points. It would suggest a hands-off approach that defers to industry and self-regulation. It also seems to suggest that existing legislation is sufficient in this regard. These points are not convincing and likely not well founded. Each point will be taken in turn.

The first point, deferring to industry and self-regulation, indicates: (1) that manufacturers can be trusted to handle this information; and (2) that the existing regulatory framework is sufficient. While the position that manufacturers can be trusted is appealing, it is unlikely to be true.[341] The FTC initially advocated for self-regulation by internet technologies, but began to provide

---

337. *Id.* at 285.

338. *See, e.g.*, Shum et al., *supra* note 2 (discussing the history of chatbots).

339. *See, e.g.*, David S. Levine, *Confidentiality Creep and Opportunistic Privacy*, 20 TUL. J. TECH. & INTELL. PROP. 11, 20-40 (2017) (discussing the intermingling between confidentiality, privacy, and trade secrets in the realm of algorithms, and associated assertions therein).

340. Some have also noted that Congress has taken a unique approach to these types of health technologies, noting that "Congress and federal regulators are facilitating rather than stifling mobile health technologies." Cortez, *supra* note 82, at 1200.

341. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1528 (2000) (noting that "industry self-regulation is at best marginally effective without legal intervention").

some degree of oversight for emerging technologies.[342] Similar to the 1990s, this period of technology includes numerous rapid developments and advancements, marked by data analytics, machine learning, and artificial intelligence.[343] With scandals and issues plaguing Mark Zuckerberg and Facebook, it is likely that public trust and confidence in website and app developers is being further eroded.[344] Public trust in technology and the advancement of these new technologies to support individuals requires legislative intervention.[345]

As regards the second point, existing law only permits the FTC to act when manufacturers engage in unfair or deceptive practices.[346] FTC action often applies to website privacy policies,[347] which are ineffective and confusing.[348] As such, these documents cannot ensure individuals are properly informed or put on notice of the uses and disclosures of their information.[349] Alternatively, the FTC could argue that, as these apps provide some form of counseling, it is implicitly deceptive to engage in uses or disclosures of information that would not be permitted by mental health professionals.[350] The FTC may not yet be willing to take this position, but some state AGs

342. *See supra* notes 123-140 and accompanying text (discussing FTC positions on regulation of the internet).

343. *See, e.g.*, Roger Parloff, *The AI Revolution: Why Deep Learning Is Suddenly Changing Your Life*, FORTUNE (Sept. 28, 2016), http://fortune.com/ai-artificial-intelligence-deep-machine-learning/.

344. Teri Robinson, *FTC confirms Facebook probe, Common Cause files two complaints against Cambridge Analytica*, SC MEDIA (Mar. 26, 2018), https://www.scmagazine.com/ftc-confirms-facebook-probe-common-cause-files-two-complaints-against-cambridge-analytica/article/753808/.

345. *Cf.* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 6 (July 1999), https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf (recommending the adoption of privacy protections for a vulnerable population due to continued growth of technology).

346. *See* 15 U.S.C. § 45 (2018); *see also* Scott, *supra* note 123.

347. Scott, *supra* note 123.

348. Amanda Grannis, Note, *You Didn't Even Notice! Elements of Effective Online Privacy Policies*, 42 FORDHAM URB. L.J. 1109, 1149-51 (2015) (discussing prior studies indicating the confusing nature of privacy policies). *See also* Joel Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J. L. & POL'Y FOR INFO. SOC'Y 485, 488-89 (2014) (noting that privacy policies are not always effective in preventing harms).

349. Grannis, *supra* note 348.

350. Gregory Klass, *Meaning, Purpose, and Cause in the Law of Deception*, 100 GEO. L.J. 449, 486-87 (2012).

may be willing to move in this direction.[351] However, this would still not provide affirmative confidentiality protections to individuals.

Further, given the complicated regulatory structure, app developers may not be sure what or how to communicate their uses and disclosures of information, or may not know whether certain laws apply to them.[352] App developers may not be aware that they are subject to federal laws, such as HIPAA or Part 2.[353] It may not be clear to consumers whether the app is voluntarily adopting those standards or is subject to them.[354] Additionally, the subtle nuances of state laws may cause consumer confusion.[355] Some uniform standard is needed for these types of apps to bring them in line with those applied to traditional mental health professionals and to prevent further confusion.[356]

A corollary to this concept is the use of the technology through multiple channels. Though not the focus of this article, it is worth noting that chatbot technology can be used either through an app or website provided by a developer, or through an existing communication channel, such as Facebook Messenger.[357] If a user engages with the developer directly, then the privacy policy of the

---

351. *Id.* The FTC has only incorporated this perspective when handling claims of false advertising and has not adopted it in the realm of privacy policies. *Id.*; *see also* Section IV.A (discussing how some state AGs have taken a more aggressive approach than the FTC).

352. *See supra* notes 148-51 and accompanying text (discussing enforcement actions against developers who have not affirmatively stated their obligations under HIPAA). *See also Mobile Tool*, *supra* note 188 (providing insight into the applicability of certain federal laws, but not encompassing all state laws).

353. *See BlueStar Privacy Policy*, WELLDOC, https://www.bluestardiabetes.com/Portal/Guest/PrivacyPolicy.htm (last accessed Apr. 30, 2018) (questioning the applicability of HIPAA). *See also supra* notes 236-240 and accompanying text (discussing how an FDA-approved mobile app geared towards substance use disorder is likely subject to SAMHSA regulations).

354. *See* J. Frazee et al., *mHealth and Unregulated Data: Is this Farewell to Patient Privacy?*, 13 IND. HEALTH L. REV. 385, 408-14 (2016) (discussing the need for a "HIPAA compliant" and a "confidential" label).

355. *See supra* notes 206-09 and accompanying text (discussing how chatbots are considered covered entities under the Texas Health Act, but nonetheless are not subject to the limitations on disclosure).

356. Frazee et al. propose a voluntary labeling mechanism to differentiate between those apps that are HIPAA-compliant, i.e., "suitable for use by covered entities and their business associates," and those that are confidential, i.e., not subject to further use and disclosure. Frazee et al., *supra* note 354, at 409. This voluntary labelling scheme is merely that—voluntary—and does not contemplate the specific types of apps discussed in this article. *Id.* at 411-12.

357. *See, e.g.*, *Frequently asked questions*, WOEBOT (last updated July 9, 2018), https://woebot.io/faqs/ ("Woebot is available on Facebook Messenger and iPhones and iPads, and Android devices!").

developer applies.[358] If a user engages with the technology through an existing communication channel, then the privacy policy of the *channel* applies.[359] This may cause consumer confusion, as individuals may switch back and forth between an app and a channel without realizing there is a difference in uses and disclosures of data.[360] This also creates a tiered system where an app developer is potentially placed at a disadvantage by trying to protect confidentiality, but the channels of communication can in essence do whatever it wants due to a broader privacy policy.[361] Regulations would alleviate these concerns.

While the arguments against heightened confidentiality requirements are worth considering, they do not reflect the practical realities of the technology or of the law. Additional regulation is necessary to promote confidentiality and to prevent unfair advantages. Without regulation as a check, the technology may not be adopted, may be adopted slowly, or may be promoted through channels without *any* restrictions on further use or disclosure, resulting in the exacerbation of mental health concerns. Thus, this regulatory scheme is not only needed, but it should be *required*, especially in light of the Facebook Cambridge Analytica scandal.[362]

C. Defining the Scope of Protections

Having identified the need for the legislation, the prior sections hint at a potential debate in terms of its scope. Legislation could focus solely on those apps that have been approved or cleared by the FDA. Alternatively, legislation could provide a more expansive view, encompassing technologies that are created, trained, or developed using cognitive behavioral therapy, regardless of their intended use.[363] This Article argues the best option is to focus only on those technologies that have been created, trained, or developed

358. *See, e.g.*, *User Privacy Policy*, WOEBOT (last updated Mar. 12, 2019), https://woebot.io/privacy.

359. *Id.* (noting that discussions "with Woebot within Facebook Messenger are subject to the Facebook Privacy Policy").

360. *Compare id.* (prohibiting all disclosures, except specific, limited examples as relates to the business), *with Data Policy*, FACEBOOK (last updated Apr. 19, 2018), https://www.facebook.com/policy.php (permitting disclosures so long as no personally identifiable information is included).

361. *Id.*

362. Robinson, *supra* note 344.

363. *Cf.* 21 U.S.C. § 321(h) (2018) (providing that a machine can be a device for purposes of FDA law based on its intended use).

using CBT, and are intended by the manufacturer or the consumer to be used in a way similar to therapists.[364]

To focus only on apps that have been approved or cleared by the FDA has a few implications. First, this assumes that the FDA is going to require approval or clearance of these chatbots and mental health apps.[365] However, the FDA has not taken any action against existing chatbots, indicating it currently does not intend to regulate them. Second, it suggests that non-approved or non-cleared devices cannot provide similar "supportive" therapies on par with those that have been approved or cleared.[366] As it stands, the creation of Woebot, Wysa, and other apps is challenging this position, which may result in changes to the position in the future. The difference between apps that have FDA approval or clearance and those that do not, alternatively, may be similar to the distinction between a psychotherapist and a social worker.[367] That is to say that one may have more rigorous training, education, and experience, but the other can still provide similar services. Finally, it may leave a wide swath of technology subject to no confidentiality requirements.[368] Apps that have not been approved or cleared would still be subject to no confidentiality requirements, even though they may provide similar services. Much of this is somewhat speculative, as it is unclear how the FDA will regulate these apps, but at least for now it does not appear they are stepping in.

To focus on the use of CBT and not the intended uses of the app would be overly broad and burdensome, encompassing additional apps in the future.[369]Individuals using Alexa or Siri may make comments such as "I'm sad" or "I'm depressed," or may ask to play music that correlate with their moods. In such instances, app developers may wish to train these technologies on cognitive behavioral therapies to offer some type of friend-like consolation.[370]

---

364. *Cf.* Gamerman, *supra* note 105 (discussing the analysis of intended use under FDA law).

365. *But see* Lee, *supra* note 65 (advocating for FDA oversight of these technologies).

366. *Id.* at 70 (noting concerns about the safety and efficacy of these technologies).

367. *See supra* notes 314-317 and accompanying text (discussing Justice Scalia's argument in *Jaffee v. Redmond* that privilege should not extend to psychotherapists).

368. *See supra* Part III (discussing how the existing regulatory framework does not provide any protections to this type of information).

369. *See* Gilman & Cooper, *supra* note 336 (advocating against excessive regulation).

370. Fitzpatrick et al., *supra* note 54 (discussing how participants using Woebot considered it to be a "friend").

However, the intent of this technology and training may not be to provide therapy or support but rather companionship.[371] As the technology would be considered "untrained app" more like a friend not subject to confidentiality protections, individuals should not have an expectation of confidentiality or privacy for the information they share, unless and until either: (1) Alexa begins to market chat/therapy offerings; or (2) users recognize and use Alexa for chat/therapy offerings. Either of these cases would encompass the technologies under the prior definition and subject them to additional confidentiality regulations. While this may prove operationally problematic for the developer, the developer has *intended* the product to be used in this manner.[372]

In light of the foregoing, the appropriate middle ground in regulating an app is to consider technology and the intended use thereof. It allows the FDA to consider whether and how to regulate these technologies, but it is not so expansive as to encompass situations that may not require confidentiality. It would also require confidentiality if other emerging technologies seek to use or leverage similar functionality. Therefore, this approach strikes the best middle-ground between advancing the technology and protecting confidentiality.

D. Enforcement of Protections

The legislation, however, requires an agency to provide oversight and enforcement. The information discussed involves mental health information, and so it would seem obvious to house enforcement authority with SAMHSA.[373] However, in the enforcement realm, SAMHSA has seen few enforcement actions over the past few years, indicating it may not have the necessary experience to conduct these investigations. By contrast, the Office of Civil Rights ("OCR") at HHS has seen an increasing numbers of enforcement actions[374] and has recently begun to enforce actions

371. *Cf.* Hoffer, *supra* note 46 (noting that chatbots can alleviate loneliness).

372. *Cf.* 21 U.S.C. § 321(h) (2018) (defining device based on "intended use"). *See also* Gamerman, *supra* note 105.

373. SAMHSA "leads public health efforts to advance the mental health of the nation." *About Us*, SAMHSA, https://www.samhsa.gov/about-us (last accessed May 1, 2018).

374. *Enforcement Highlights*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (last accessed Mar. 6, 2018) (noting resolution of over 25,695 cases, with settlements and penalties equaling over $75 million).

against business associates and technology vendors.[375] In a similar fashion, the FTC has worked on a number of cases involving technology providers[376] and has coordinated with OCR since at least 2008.[377] AGs can also take action in this area through enforcement of HIPAA.[378] Given the focus on investigations of technologies, privacy enforcement, and the existing concurrent jurisdiction between aforementioned entities, this framework seems well-suited to provide continued oversight of these new technologies. OCR, FTC, and AGs should be given the tools to enforce this new legislation.[379]

VI. CONCLUSION

Apps and technology are changing how people live their lives and how healthcare is practiced. Machine learning, artificial intelligence, and data analytics are altering how people can chat and receive support, akin to traditional therapy forms. While these new technologies are certainly no substitute for consumers facing long-term depression, anxiety, or other more serious issues, they can help support individuals who may prefer to use texting or written communication to therapy. They may also alleviate long-held stigmas about mental health issues and treatment. However, without appropriate confidentiality regulations, chatbots and other software-based therapy apps fail to maintain the same degree of confidence and trust that traditional therapy or counseling may maintain. Thus, new legislation is necessary to provide adequate confidentiality

375. *See, e.g.*, *$2.5 million settlement shows that not understanding HIPAA requirements creates risk*, HHS.GOV (Apr. 24, 2017), https://www.hhs.gov/about/news/2017/04/24/2-5-million-settlement-shows-not-understanding-hipaa-requirements-creates-risk.html ("This settlement is the first involving a wireless health services provider.").

376. *See, e.g.*, Beales, *supra* note 116.

377. *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Consumers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations*, FED TRADE COMM'N, (Feb. 18, 2009), https://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial.

378. Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 46 LOY. U. CHI. L.J. 175, 212-215 (2014) (advocating for greater cohesion between OCR and state AGs).

379. Congress seemed to hint at this as a framework as part of the HITECH Act, when it requested the FTC and HHS to discuss privacy matters. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, § 13407, 123 Stat. 269-70 (2009). These organizations have already collaborated on guidance for mobile application developers in healthcare as well. *See Mobile Tool*, *supra* note 188.

protections for this information. This inquiry, however, does not end here: as these technologies continue to change and evolve, we must remain ever vigilant in protecting individual privacy and confidentiality.