TULANE JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY

VOLUME 24 SPRING 2022

Assessing Anonymity: Privacy in Online Mental Healthcare and Support Groups

Nick Feldstern*

Confusion surrounding data privacy laws and the vulnerable cybersecurity of many major technology platforms has created an environment where those most in need of remote mental healthcare are uncomfortable seeking it. The methods of digital treatment that cropped up during the COVID-19 pandemic proved effective and are likely here to stay long after a return to normalcy. While there will always be a market for in-person therapy and support groups, the increase in access to mental healthcare is simply too beneficial to ignore. This Article examines the patchwork of federal and state privacy laws and proposes that the current system is insufficient to sustain the expansion of remote mental healthcare. Until the federal government develops a more robust digital privacy scheme, state legislators and technology developers alike must consider the privacy needs of those seeking mental health treatment through professional services and online support groups.

* © 2022 Nick Feldstern. J.D. 2021, George Washington University Law School; BA in History, 2017, University of California, Santa Barbara. Mr. Feldstern is clerking at the United States Civilian Board of Contract Appeals, assisting the Board with the adjudication of federal contract disputes. The author would like to thank Professor Dawn Nunziato for her support and encouragement throughout the drafting of this article.

I. INTRODUCTION

Jane is a forty-two year-old recovering alcoholic. She has found great success with the Alcoholics Anonymous (AA) program and has been sober for over five years. In the past, Jane frequently turned to alcohol when she experienced depression, but now, with the help of in-person support groups like AA, she has found healthy alternatives to promote her mental health. Now, Jane is stuck at home. She watches the news daily as the COVID-19 pandemic sweeps across the world. She is told to stay away from public gatherings and her job has fortunately allowed her to work from home. She has several friends with whom she has remained in contact, but she only sees them once every few weeks during a Zoom video conference when their schedules allow it.

Jane begins to feel her depression returning. She is unable to engage in some of her more social coping mechanisms and is unable to meet with her in-person AA support group. Instead, Jane searches the Internet for similarly situated individuals and seeks virtual alternatives to her typical support systems. She discovers that many like her have signed up for virtual therapy sessions with licensed mental health professionals. She finds others who have conducted or participated in AA meetings via Zoom.

Jane, a veteran of the AA program, recalls the sensitive information often discussed during these programs. She is uncomfortable with the idea of recording herself sharing her most intimate history and is afraid of the consequences to her life if those details were made public. The idea of sitting in front a camera, even under a fake username, seems to go against the goal of anonymity. Many members of her family do not know about her past with addiction and her job is certainly unaware. She has seen on the news that companies like Zoom, Facebook, and Skype all have

questionable track records of data security, but she does not quite understand how data security works in the first place. But she knows she is headed toward trouble, so what is she to do?

While this is a fictional anecdote, countless Americans are experiencing issues similar to those of Jane. The COVID-19 pandemic has created a mental health crisis unlike anything before seen in America, and while promising technologies have emerged to combat the crisis, risk to data security has never been higher. The confusing patchwork of federal and state digital privacy laws combined with an unprecedented increase in data breaches serve to discourage those in need of mental health treatment from seeking online alternatives. This Article seeks to survey the landscape of virtual privacy in the context of remote mental healthcare and to hopefully provide guidance in crafting better policies to encourage more participation in mental health treatment.

Part II provides background on the history of telemedicine, how telemedical technology applies to mental healthcare and online support groups, and how the COVID-19 pandemic has brought about a massive increase in teletherapy. It discusses why digital privacy concerns are so prevalent within the teletherapy industry and how patient information is collected, shared, and utilized. Part III examines the current legal framework for digital privacy on both the federal and state level, including initiatives to strengthen current regimes that have emerged in the past year. Currently, California leads the pack on digital privacy reform, but initiatives from states like Virginia and Florida appear promising. Part IV looks at ongoing litigation relevant to the collection of personal information by technologies that have been used for remote mental healthcare. Finally, Part V looks forward to the future of mental healthcare and how patients and platforms can best prepare for a world where therapy is a click away.

II. BACKGROUND

The medical use of telecommunication technology dates back nearly to the technology's inception. Not long after Alexander Graham Bell patented the telephone, fantasies of telemedicine emerged in the American popular culture.[1] In 1924, three years before the first television transmission, a magazine depicted a "radio doctor" capable of

1. MARILYN J. FIELD, TELEMEDICINE: A GUIDE TO ASSESSING TELECOMMUNICATIONS FOR HEALTH CARE 35 (1996) [hereinafter Telemedicine Guide].

communicating in live picture with his patient.[2] A quarter century later, telemedicine first emerged in medical literature in an article discussing the transmission of radiologic images over twenty-four miles away.[3] The medical use of video communication dates back to 1959; and in 1967, the University of Nebraska established a "telemedicine link" with a hospital 112 miles away for the purposes of "speech therapy, neurological examinations, diagnosis of difficult psychiatric cases, case consultations, research seminars, and education and training."[4]

Many early applications of telemedicine arose out of the need for medical access in rural and remote areas, but its use proliferated in urban locales as well.[5] In the late 1960s, the federal government, led by the U.S. Department of Health, Education, and Welfare (now the Department of Health and Human Services); the Department of Defense; and NASA, began investing substantial resources into the research and application of telemedicine.[6]

Today, telemedicine has become an integral facet of the healthcare system, allowing patients to remotely receive care, consult with providers, get information about a condition or treatment, arrange for prescriptions, and receive diagnoses.[7] Telemedicine expands access to rural, underserved, and vulnerable populations that would not otherwise receive high quality healthcare.[8] Popular methods of telemedicine include virtual visits, chat-based interactions, and remote patient monitoring.[9]

While telemedicine is highly valued within traditional medical fields, it has likewise proven extraordinarily effective in the field of mental and psychological healthcare.[10] A 2019 study found that nearly one in five American adults live with mental illness and less than half seek treatment.

---

2. *Id.* at 35-36.
3. *Id.* at 36.
4. *Id.*
5. *See id.* at 38.
6. *See id.* at 39.
7. *Telehealth: Defining 21st Century Care*, AM. TELEMEDICINE ASS'N, http://www.americantelemed.org/resource/why-telemedicine (last visited Mar. 12, 2021).
8. *Id.*
9. *Id.*
10. *See* Lawrence Gleit, *The Role of Telemedicine in Mental Health*, HEALTH IT OUTCOMES (June 19, 2017), http://www.healthitoutcomes.com/doc/the-role-of-telemedicine-in-mental-health-0001.

[11, 12] Studies suggest telepsychology is as effective, if not more so, than its face-to-face counterpart, and the increased access and flexibility lead to more patient engagement with treatment.[13] Remote mental healthcare takes many forms, including telephone calls, video conferences, email correspondences, chat rooms, and smartphone applications.[14] One of the earliest examples of an online counseling service is Dear Uncle Ezra, an online advice column created in 1986 by Cornell University and operated for twenty-six years.[15]

In addition to professional mental health treatment, online support groups are an invaluable resource for those suffering from addiction, trauma, and other physical or psychological hardships. The American Society of Addiction Medicine provides a directory for a variety of support groups and resources to promote recovery and ensure confidentiality.[16] The National Network to End Domestic Violence states "[o]nline support groups can be a valuable way . . . for survivors to connect with support and other survivors when they are not able to meet in person."[17]

Privacy, confidentiality, and anonymity are of paramount concern within both professional mental healthcare and online support groups. The quintessential confidential relationship between psychologist and patient is necessary to foster trust, communication, and healing.[18] Anonymity is of particular importance for those seeking substance abuse treatment and those suffering from domestic violence.[19] The risk of being identified may

---

11. Substance Abuse and Mental Health Services Administration [SAMHSA], *2019 National Survey of Drug Use and Health (NDHSU) Releases*, tbl. 8.1A, HEALTH & HUMAN SERV., http://www.samhsa.gov/data/release/2019-national-survey-drug-use-and-health-nsduh-releases.

12. *Mental Illness*, NAT'L INST. OF MENTAL HEALTH, http://www.nimh.nih.gov/health/statistics/mental-illness.shtml (last visited Jan. 2021).

13. *See* Gleit, *supra* note 10; *see also* Nicole Owings-Fonner, *Research Roundup: Telehealth and the Practice of Psychology*, AM. PSYCHOL. ASS'N (Oct. 2018), http://www.apaservices.org/practice/ce/expert/telehealth-practice-psychology.

14. *See* Owings-Fonner, *supra* note 13.

15. *See* Susan S. Lang, *For Two Decades, Dear Uncle Ezra, World's First Online Advice Column, Has Aided the Perplexed, the Shy and the Confused*, CORNELL CHRON. (Feb. 20, 2007), http://news.cornell.edu/stories/2007/02/any-person-any-question-ask-dear-uncle-ezra-advice.

16. *See Promoting Support Group Attendance*, AM. SOC'Y ADDICTION MED., http://www.asam.org/Quality-Science/covid-19-coronavirus/promoting-support-group-attendance (last visited Mar. 12, 2020).

17. Nat'l Network to End Domestic Violence, *Online Support Groups for Survivors*, TECH. SAFETY (2020), http://www.techsafety.org/online-groups.

18. *See* Kristin Kelley, *Is Telepsychology Putting Our Most Vulnerable Patients at Risk?*, 15 J. HEALTH & BIOMEDICAL L. 55, 63 n.50 (2019) (citing *Confidentiality*, PSYCHOL. INFO., http://psychology-info.com/confidentiality).

19. McCarton Ackerman, *Why is Anonymity Important in Addiction Recovery?*, AM. ADDICTION CTRS. (Dec. 18, 2019), http://www.recovery.org/why-is-anonymity-important-in-addiction-recovery ("For the recovering addict, anonymity allows for a safe space to open up to

be an insurmountable deterrent for those seeking help. Support groups such as Alcoholics Anonymous, Anxiety and Depression Association of America, and the National Domestic Violence Hotline maintain strict confidentiality and anonymity policies.[20] As these services transition to virtual platforms, privacy emerges as a paramount issue surrounding remote mental healthcare.[21]

In addition to privacy and confidentiality concerns, mental healthcare professionals highlight other impediments not traditionally present during face-to-face treatment. Minute physical cues—knotted hands, tapping feet, shifting around—are often invaluable for treating patients.[22] These cues are often lost over a video conference and are entirely absent in other forms of teletherapy.[23] Similarly, patients struggling with substance abuse often exhibit signs of use that are easier to disguise during a virtual conversation.[24] Patients may also be less inclined to share honestly with therapists over the Internet.[25] In addition to privacy concerns, virtual therapy lacks the intimacy that encourages open and honest conversation.[26]

---

others and address issues they wouldn't feel as comfortable discussing in a more public setting."); Sara Baker, *Why Online Anonymity is Critical for Women*, WOMEN'S MEDIA CTR. (Mar. 11, 2016), http://www.womensmediacenter.com/speech-project/why-online-anonymity-is-critical-for-women ("Privacy allows survivors to live without the constant fear that their abuser is watching their every step or lurking behind every corner, as abusers use surveillance to create such fear.").

20. *Understanding Anonymity*, ALCOHOLICS ANONYMOUS 5 (June 2019), http://www.aa.org/sites/default/files/literature/assets/p-47_understandinganonymity.pdf ("Anonymity is the spiritual foundation of all our traditions, ever reminding us to place principles before personalities."); *Terms of Use*, ANXIETY & DEPRESSION ASS'N OF AM. (Nov. 19, 2020), http://adaa.org/terms-of-use ("ADAA promotes privacy and encourages participants to keep personal information such as address and telephone number from being posted. Similarly, do not ask for personal information from other participants. Any comments that ask for telephone, address, e-mail, surveys and research studies will not be approved for posting."); *Privacy Policy*, NAT'L DOMESTIC VIOLENCE HOTLINE, http://www.thehotline.org/privacy-policy/ (last visited Mar. 12, 2020) ("The National Domestic Violence Hotline defines anonymous communication as a onetime individual contact where digital services are provided between a chatter and advocate in which no information is collected that can connect the user to the individual service interaction.").

21. *See, e.g.*, Chloe Hadavas, *Why You Shouldn't Just Skype Your Therapist*, SLATE (Mar. 17, 2020, 6:26 PM), http://slate.com/technology/2020/03/coronavirus-pandemic-therapy-online-teletherapy.html.

22. *See* Jeffrey Kluger, *Online Therapy, Booming During the Coronavirus Pandemic, May Be Here to Stay*, TIME (Aug. 27, 2020, 8:00 AM), http://time.com/5883704/teletherapy-coronavirus.

23. *See id.*

24. *See id.*

25. *See id.*

26. *See id.*

A. How Personal Information is Collected and Shared by Online Therapy Applications

The market for online therapy applications has boomed over the last several years as smartphone and social media technology flourished.[27] Many services offer on-demand therapy sessions via text, call, or video chat with licensed counselors, and most of the leading applications boast full compliance with applicable privacy laws.[28] Despite an outward concern for user privacy, studies into the collection and dissemination of mental health data cast an entirely different light upon online therapy applications.[29]

In order to understand the problem, it is perhaps best to begin with an example illustrating how mental health information can be collected, shared, and utilized. Reporters for the website Jezebel conducted a study by signing up for the popular therapy application, BetterHelp, and monitoring its data collection.[30] The developers of BetterHelp claim to be "totally obsessed about ensuring your privacy and confidentiality" through "state-of-the-art" encryption and rigid privacy policies.[31] No matter how "totally obsessed" the developers may be, the realities of internet advertising and social media interconnectivity means sensitive information does funnel through the application, "all with the ostensible goal of better tracking user behavior, and perhaps giving social media companies an easy way to see who's feeling depressed."[32]

While health privacy laws like the Health Information Portability and Accountability Act (HIPAA) prevent BetterHelp from sharing identifiable information, no law prevents the application from alerting Facebook each time a user talks to their therapist, or sharing a user's "pseudo-anonymous" feelings about depression or addiction with analytics companies.[33] Upon first downloading BetterHelp, users are presented with a survey that catalogs "gender, age, and sexual orientation, along with more specific

---

27. *See* Molly Osberg & Dhruv Mehrotra, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020, 1:39 PM), http://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137.

28. *See id.*

29. *See* Kit Huckvale et al., *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, JAMA NETWORK (Apr. 19, 2019), http://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=041919.

30. *See* Osberg & Mehrotra, *supra* note 27.

31. *Frequently Asked Questions*, BETTERHELP, http://www.bcms.org/lifebridge/faq/Confidentiality.pdf (last visited Apr. 28, 2021).

32. Osberg & Mehrotra, *supra* note 27.

33. *See id.*

areas of concern, like the last time a person had suicidal thoughts or if they'd ever been to therapy before."[34] The investigation found that BetterHelp immediately began informing companies like Facebook, Google, Pinterest, and Snapchat that the user was considering treatment and would send metadata from every message between patient and therapist.[35] Although the contents of the messages remained confidential, the social media companies could know the time of day, approximate location, and length of the session.[36]

BetterHelp shared even more information with the research and analytics firm MixPanel.[37] Though anonymized per HIPAA requirements, "[r]esearch suggests that even when information like this is collected by hospitals or insurance providers, it's often quite easy to match it back to an individual patient."[38] According to the Jezebel reporters, "MixPanel knew where we were and what device we were using; approximately how old we were, whether we considered ourselves spiritual or religious, our financial status, and our sexual orientation."[39] MixPanel and other data analytics companies collect this information to produce monetizable data out of any individual's internet behavior, and mental health data is perhaps the most valuable.[40]

A more expansive study conducted by the JAMA Network recorded similar results.[41] An assessment of the privacy policy content and data transmission among the thirty-six top-ranked applications for depression and smoking cessation found that "[d]ata sharing with third parties that includes linkable identifiers is prevalent and focused on services provided by Google and Facebook" and that "users are denied an informed choice about whether such sharing is acceptable. . . ."[42]

The two studies highlight the immense gaps in online privacy regulations and the need for legislation applicable to modern technology. Notably, both studies were conducted prior to the COVID-19 outbreak.[43] In the past year and a half, a dramatic increase in online therapy has

---

34. *Id.*
35. *See id.*
36. *See id.*
37. *See id.*
38. *Id.* (citing Ji Su Yoo, *Study Finds HIPAA Protected Data Still at Risks*, HARV. GAZETTE (Mar. 8, 2019), http://news.harvard.edu/gazette/story/newsplus/study-finds-hipaa-protected-data-still-at-risks).
39. *Id.*
40. *See id.*
41. *See* Huckvale et al., *supra* note 29.
42. *Id.*
43. *See id.*; *see also* Osberg & Mehrotra, *supra* note 27.

brought about an abundance of privacy concerns.[44] The COVID-19 pandemic and its year-long quarantine has engendered a mental health crisis unprecedented in modern American history.[45] Many of those suffering the detrimental effects of isolation have no alternative but to turn to remote mental healthcare.[46]

B. Online Therapy and Support Groups Become the New Normal During the COVID-19 Pandemic

The psychological burdens caused by the pandemic, including "social isolation, widespread unemployment, worries over contracting the virus, insomnia, social media exposure, and the rising death toll[,]" cannot be overstated.[47] Worldwide, psychological studies have documented an increase in mental health deterioration including depression, anxiety, stress, and suicidality.[48] Social isolation and other stressors also contribute to cognitive decline and substance abuse.[49] Like so many social ills, the mental health effects of COVID-19 have disproportionately impacted vulnerable groups, "such as older adults, racial and ethnic minorities, people living with disabilities, people who are neurologically atypical, children, and people who are homeless."[50]

Due to the nature of infectious disease, the mental healthcare field experienced a rapid and unavoidable transition toward digital therapy and online mental health applications.[51] Some in the profession praise the benefits of remote therapy, such as broader access, but others are wary of the dangers associated with online technology, such as privacy and data protection.[52] While many areas of telemedicine are heavily regulated, remote mental healthcare is often subject to less stringent regulation,

---

44. *See* Complexity of Internet Privacy Law, *infra* Part II(C).

45. *See* Nicole M. Martin et al., *Ethics of Digital Mental Health During COVID-19: Crisis and Opportunities*, JMIR PUBL'N (Dec. 22, 2020), http://mental.jmir.org/2020/12/e23776/.

46. *See id.*

47. *Id.*

48. *See* Yasmin Tayag, *Who's Most at Risk in the Covid-19 Mental Health Crisis*, MEDIUM CORONAVIRUS BLOG (Sept. 21, 2020), http://coronavirus.medium.com/whos-most-at-risk-in-the-covid-19-mental-health-crisis-2f1ddd5bba9c; *see also* Jianyin Qiu et al., *A Nationwide Survey of Psychological Distress Among Chinese People in the COVID-19 Epidemic: Implications and Policy Recommendations*, GENERAL PSYCHIATRY (Feb. 29, 2020), http://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC7061893&blobtype=pdf.

49. *See* Martin et al., *supra* note 45.

50. *Id.*

51. *See id.*

52. *See* Olga Khazan, *Why Your Shrink Wasn't Offering Virtual Therapy Until Now*, ATLANTIC (May 12, 2020, 6:26 PM), http://www.theatlantic.com/health/archive/2020/05/virtual-therapy-pandemic/611551; *see* Hadavas, *supra* note 21.

especially in the context of non-professional programs and support groups. For example, as the section below will elaborate, HIPAA does not apply to information shared among support group members.[53]

Both the federal government and state governments have loosened regulations on telehealth platforms during the pandemic.[54] This development has allowed many tech companies to enter the arena of telemedicine and there now exists more platforms for remote mental healthcare than ever before.

C. Dominant Platforms in the Digital Mental Healthcare Field

As Americans' lives shifted online, video conferencing and social media platforms became the dominant form of personal, professional, and social interaction.[55] Among them, the video conferencing platform Zoom emerged as a household name and quickly became the most popular application for business, education, and, in some cases, medicine.[56] Zoom and other platforms, including FaceTime, Skype, and Doxy, allow doctors to interact with patients over video chat for non-emergency situations.[57] These interactions are helpful for routine medical complaints and for those hesitant to seek in-person medical treatment for fear of contracting COVID-19.[58] However, due to the confidential nature of medical information, the security of these platforms has been under enormous scrutiny.[59]

Zoom and other video conferencing platforms have also dominated the mental healthcare field and are commonly used for support groups.[60] Like other medical fields, confidentiality and privacy in mental health is an utmost concern.[61] But, unlike other medical fields, many government regulations do not apply.[62] This lack of regulation can lead to hesitancy in

---

53. *See* Elizabeth Litten, *Patient Support Groups, Email and the Duty to Warn*, FOX ROTHSCHILD (Nov. 5, 2014), http://hipaahealthlaw.foxrothschild.com/2014/11/articles/privacy/patient-support-groups-email-and-the-duty-to-warn.

54. *See* Relevant Litigation, *infra* Part IV.

55. *See* Natalie Sherman, *Zoom Sees Sales Boom Amid Pandemic*, BBC (June 2, 2020), http://www.bbc.com/news/business-52884782.

56. *See id.*

57. *See* Brian Turner & Jonas P. DeMuro, *Best Telemedicine Software of 2021*, TECH RADAR (May 28, 2021), http://www.techradar.com/best/best-telemedicine-software.

58. *See id.*

59. *See, e.g.*, Drew Harwell, *Thousands of Zoom Video Calls Left Exposed on Open Web*, WASH. POST (Apr. 3, 2020), http://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web.

60. *See* Kluger, *supra* note 22.

61. *See* Federal Privacy Law, *supra* Part III(A).

62. *See* State Privacy Law, *supra* Part III(B).

those seeking mental health treatment over a digital application.[63] Zoom in particular has experienced several data breaches and has been embroiled in serious litigation surrounding its data security.[64]

Telehealth is subject to a complex web of medical and digital privacy law.[65] Currently, digital privacy law is a patchwork of federal and state laws, leading to much confusion in the field, and the dramatic increase in digital healthcare has generated many novel legal issues.[66] The next Part expands on medical and digital privacy law on both the federal and state level, including current initiatives seeking to increase data privacy rights and further regulate online platforms.

III. LEGAL FRAMEWORK FOR DIGITAL PRIVACY

Understanding digital privacy law in America is a lesson in federalism and an example of how a vacuum of federal authority can create an indiscernible web of state regulations. Courts and agencies have applied various federal laws to address cybersecurity issues, but there exists no single statute directly concerned with federal digital privacy protection.[67] Instead, states have taken it upon themselves to ensure data security for their citizens by enacting a variety of regulations that take many different forms.[68] This Part expands on applicable federal privacy law and how federal agencies such as the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) attempt to set national privacy standards. It then turns to the state initiatives that currently lead the way in privacy legislation.

If this Part confuses the reader, it is because privacy law in America is complex, messy, and presents a near insurmountable barrier for those seeking to understand it. An individual seeking remote mental health treatment with even a minor understanding of data security risks can seek no refuge in the current landscape of American digital privacy law. Only by establishing uniform privacy standards and comprehensible cybersecurity legislation will those individuals feel safe to share their most intimate information.

---

63. *See* Osberg & Mehrotra, *supra* note 27.
64. *See* Harwell, *supra* note 59.
65. *See* Relevant Litigation, *infra* Part IV.
66. *See id.*
67. *See* Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Apr. 2, 2021). http://www.varonis.com/blog/us-privacy-laws.
68. *See, e.g.*, California Consumer Privacy Act of 2018 [CCPA], Cal. Civ. Code §§ 1798.100-1798.199 (effective Jan. 1, 2020), available http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

A. Federal Privacy Law

Compared to more robust state privacy laws, federal law provides relatively little in terms of data privacy protection. Patients seeking professional mental healthcare are likely protected under federal laws securing medical information, but many other avenues of treatment, such as online support groups, may not qualify for such protection.[69] Further, not all platforms utilized for digital therapy are compliant with federal privacy statutes.[70] This complexity may discourage those seeking treatment from sharing pertinent personal information or put an unwary patient at risk of serious data theft.[71]

1. HIPAA and Mental Healthcare

The principal statute protecting medical information is the Health Information Portability and Accountability Act.[72] Enacted in 1996, HIPAA sought to "modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and to address limitations on healthcare insurance coverage."[73] The statute seeks to safeguard patient information created, stored, or transmitted by or on behalf of "covered entities," including most healthcare providers.[74]

Among its many moving parts, HIPAA operates primarily based on two rules issued by HHS. The Privacy Rule creates national standards for the use and disclosure of Protected Health Information (PHI)—how and when healthcare professionals, lawyers, or anyone who accesses your PHI can or cannot use that data.[75] The Security Rule establishes a national set

---

69. *See* Martin et al., *supra* note 45.

70. *See* Brandon Vogel, *Telehealth via TikTok is Not Protected Under HIPAA, but Zoom Is: What Attorneys Need to Know About Mental Health Apps*, N.Y. STATE BAR ASS'N (Dec. 11, 2020), http://nysba.org/telehealth-via-tiktok-is-not-protected-under-hipaa-but-zoom-is-what-attorneys-need-to-know-about-mental-health-apps.

71. *See* Osberg & Mehrotra, *supra* note 27; *see also* Rachel Becker, *That Mental Health App Might Share Your Data Without Telling You*, VERGE (Apr. 20, 2019, 12:05 PM), http://www.theverge.com/2019/4/20/18508382/apps-mental-health-smoking-cessation-data-sharing-privacy-facebook-google-advertising.

72. *See generally* Health Insurance Portability and Accountability Act of 1996 [HIPPA], Pub. L. 104-91, 110 Stat. 1936 (1996).

73. *HIPAA for Dummies*, HIPAA GUIDE, http://www.hipaaguide.net/hipaa-for-dummies (last visited Mar. 13, 2020) [hereinafter HIPPA For Dummies].

74. *See* 45 C.F.R. § 164.306.

75. *Summary of the HIPAA Privacy Rule*, HEALTH & HUMAN SERVS. (July 26, 2013), http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

of security standards for protecting certain health information that is held or transferred in electronic form.[76]

The key question for both patients seeking mental health treatment and platforms offering remote therapy tools is what counts as a "covered entity." The HIPAA rules only apply to "covered entities," so any information shared to an uncovered entity or an uncovered platform is not protected by HIPAA.[77]

Adding to the complexity, in March 2020, the HHS Office of Civil Rights (OCR) announced it would relax HIPAA enforcement and issued new guidance to encourage the participation of companies in the fight against COVID-19.[78] The OCR has exercised its enforcement discretion to not impose penalties on telehealth providers for HIPAA violations "in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency."[79] This discretionary nonenforcement also includes good faith disclosure of PHI to public health officials.[80] It applies only to "non-public facing" remote communication products, including video conference platforms like Zoom and other telehealth technologies.[81]

Essentially, the rule change has rendered a large swath of previously protected PHI unprotected under HIPAA, including information stored and disseminated through many digital tools used for mental healthcare.[82] Combined with the "covered entities" question, it has become significantly complicated to determine whether information shared in the process of remote mental healthcare is protected or not.

---

76. *Id.*

77. *See* HIPAA For Dummies, *supra* note 73.

78. *See Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, HEALTH & HUMAN SERVS. (last reviewed Jan. 20, 2021), http://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html [hereinafter Notification of Enforcement Discretion for Telehealth Remote Communications].

79. *Id.*

80. *OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During the COVID-19 Nationwide Public Health Emergency*, HEALTH & HUMAN SERVS. Apr. 2, 2020), http://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html.

81. Notification of Enforcement Discretion for Telehealth Remote Communications, *supra* note 78.

82. *See* Martin et al., *supra* note 45.

2. Other Federal Privacy Laws

Beyond HIPAA, the federal government has little in the way of digital privacy enforcement. Under the Federal Trade Commission Act of 1914, the FTC may bring enforcement action against companies for engaging in "unfair or deceptive acts or practices. . . ."[83] The FTC may not bring an unfairness action "unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[84] This authority has been exercised against leading tech and social media companies for their collection, storage, and dissemination of user data, as well as data breaches.[85] While enforcement is typically limited to whether the company's use of user data comports with its own privacy policies, two cases suggest "unfairness" may apply where a company's security safeguards are insufficient.[86]

In *F.T.C. v. Wyndham Worldwide Corp.*, the FTC alleged Wyndham engaged in unfair and deceptive cybersecurity practices that resulted in three separate data breaches, compromising over half a million customers.[87] Although the FTC had previously asserted "unfairness" as a grounds to regulate cybersecurity practices, *Wyndham* became the first real challenge to the breadth of this authority.[88] The Third Circuit examined whether the FTC has authority to regulate cybersecurity under the unfairness prong of 15 U.S.C. § 45(a).[89] Following a meticulous inquiry into the FTC's regulatory authority, the Third Circuit rejected *Wyndham*'s arguments that the "unfairness" prong should be narrowly construed as not to apply.[90] The court wrote, "the relevant inquiry here is a cost-benefit analysis" that considers factors, including "the probability and expected size of reasonably unavoidable harms to consumers given a certain level

83. 15 U.S.C. § 45(a); *see also A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, *Fed. Trade Comm'n*, (revised May 2021) http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

84. 15 U.S.C. § 45(n).

85. *See* Green, *supra* note 67.

86. *See id.*; *see also* F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 244-49 (3d Cir. 2015); LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1227 (11th Cir. 2018).

87. *See Wyndham*, 799 F.3d at 240.

88. *See* Matthew Nelson, *The Global Impact of FTC v. Wyndham: Another Reason Your Company Should Review Its Privacy and Cybersecurity Programs Right Now*, 34 No. 1 ACC Docket 50, 52 (2016).

89. *See Wyndham*, 799 F.3d at 240.

90. *See id.* at 24-49.

of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[91]

The opinion fell short of plainly establishing the FTC's authority to regulate cybersecurity under unfairness actions for several reasons. First, the Third Circuit contextualized its opinion solely on the factual circumstances presented, diminishing the opinion's analogical value.[92] Second, the cost-benefit analysis appears to allow companies the discretion to decide whether additional cybersecurity measures make good business sense.[93] Finally, as a circuit court opinion, *Wyndham* left open the possibility of other circuits ruling differently.[94]

Indeed, nearly three years later, the FTC again alleged that an inadequate data-security program constituted an "unfair act or practice" under Section 45(a).[95] In *LabMD, Inc. v. F.T.C.*, an employee at a medical laboratory installed a peer-to-peer file-sharing program on a company computer, allowing the exfiltration of 1,718 pages of patient information by a cybersecurity company seeking to solicit LabMD's business.[96] The FTC issued a broad cease and desist commanding LabMD to overhaul and replace its data-security program.[97] The Eleventh Circuit validated the FTC's authority to regulate cybersecurity under Section 45(a), but vacated the FTC's cease and desist because the prohibitions contained within lacked specificity.[98] Both *Wyndham* and *LabMD* are consistent and should be read together, but *LabMD* established a high bar for the FTC to pursue an "unfairness" action. [99]

Other federal privacy statutes include the U.S. Privacy Act of 1974, the Children's Online Privacy Protection Act (COPPA), which regulates the collection of data from minors, and the Gramm-Leach-Bliley Act (GLBA), aimed at securing financial and banking information.[100] Neither of these statutes, with the exception of COPPA in the context of minors seeking remote mental healthcare, are particularly helpful for protecting data collected during teletherapy or online support groups. Instead,

---

91. *Id.* at 255.
92. *See* Nelson, *supra* note 88.
93. *See* Almudena Arcelus et al., *How Much is Data Security Worth*, 15 SCITECH L. 10, 12 (2019).
94. *See* Nelson, *supra* note 88, at 53.
95. *See* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1223-24 (11th Cir. 2018).
96. *See id.* at 1224.
97. *See id.* at 1236.
98. *See id.*
99. *Cf.* F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 239 (3d Cir. 2015), *with LabMD*, 894 F.3d at 1221.
100. 5 U.S.C. § 552a; *see* 15 U.S.C. §§ 6501-05, 6801.

protection may be found under state privacy regulations, which have been substantially more comprehensive than their federal counterparts.[101]

3. Federal Privacy Initiatives During COVID-19

In response to the growing mental health crisis, the Food and Drug Administration (FDA) relaxed regulations on mental health applications to "expand the availability of digital health therapeutic devices."[102] While this certainly broadens access to mental healthcare, lowering standards for the technology may lead to a "substandard tier of service."[103] Indeed, such loosening of regulation "opens the gate for unvetted apps and other services that are put on the market purely for profiteering off of the ongoing mental health crisis rather than providing actual relief for patients."[104]

Additionally, HHS expanded access to Medicare telehealth services so that beneficiaries can receive a wider range of remote healthcare.[105] According to the policy, "[a] range of providers, such as doctors, nurse practitioners, clinical psychologists, and licensed clinical social workers, will be able to offer telehealth to their patients."[106] While this is certainly beneficial for those seeking professional mental healthcare, it omits many common forms of treatment such as group therapy and support groups.

B. State Privacy Law

1. California

California is leading the pack in internet privacy legislation. As the hub of many of the world's top social media and technology companies, California is in a unique position to dictate the future of digital privacy and has taken it upon itself to ensure the data security of California residents.

---

101. *See* Allison Grande, *Va. Becomes 2nd State to Enact Consumer Privacy Law*, LAW360 (Mar. 2, 2021) http://www.law360.com/articles/1360772/print?section=compliance.

102. *Enforcement Policy for Digital Health Devices for Treating Psychiatric Disorders During the Coronavirus Disease 2019 (COVID-19) Public Health Emergency*, FOOD & DRUG ADMIN. (Apr. 2020), http://www.fda.gov/media/136939/download.

103. Martin et al., *supra* note 45.

104. *Id.*

105. *Medicare Telemedicine Health Care Provider Fact Sheet*, CTR. MEDICARE & MEDICAID SERVS. (Mar. 17, 2020), http://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet.

106. *Id.*

Due to the global nature of big technology, California policy often has a widespread and significant impact on users across the world.[107]

In January 2020, the California Consumer Privacy Act (CCPA) went into effect and marked a notable shift in the collection and dissemination of user information.[108] The Act seeks to increase transparency in data collection and give Californians more control over how companies use and share their personal information.[109] Under the CCPA, Californians have the right to request information from companies concerning the collection and use of their data, the right to have that information deleted, and the right to restrict future collection and sale of personal data.[110] The California attorney general has the authority to bring action against any noncompliant company.[111]

In November 2020, Californians voted in favor of the California Privacy Rights and Enforcement Act (CPRA), which amended the CCPA to create an entirely new enforcement agency and close loopholes present in the CCPA.[112] Although the Act does not go into effect until 2023, tech companies will likely alter their platforms in preparation for the change.

In response to COVID-19, California loosened restrictions under the CCPA for the dissemination of certain forms of "deidentified health data" to aid in research.[113] The information may be shared, so long as it is "(1) deidentified under HIPAA; (2) derived from medical information; and (3) not subsequently reidentified."[114]

2. Other States

Although none are as far-reaching as the combined CCPA and CPRA, other states have enacted data privacy and consumer protection laws. Maine's "Act To Protect the Privacy of Online Customer

---

107. *See* Carolyn W. Martin & Nick Feldstern, *Raising the Bar for Internet Privacy: California's Proposition 24*, LUTZKER & LUTZKER (Nov. 4, 2020), http://www.lutzker.com/raising-the-bar-for-internet-privacy-californias-proposition-24/.

108. *See* California Consumer Privacy Act, *supra* note 68.

109. *See id.*

110. *Id.*

111. *Id.*

112. *See* Paul W. Sweeney et al., *California Voters Approve (Another) Overhaul of California Consumer Privacy Laws: Meet the California Privacy Rights Act*, NAT'L L. R. (Jan. 13, 2021), http://www.natlawreview.com/article/california-voters-approve-another-overhaul-california-consumer-privacy-laws-meet.

113. Alexander H. Southwell et al., *U.S. Cybersecurity and Data Privacy Outlook and Review—2021*, GIBSON DUNN (Jan. 28, 2021), http://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2021/; *see* Cal. Civ. Code §§ 1798.130(a)(5)(D), 1798.146, 1798.148.

114. Southwell et al., *supra* note 113.

Information" prohibits the use, disclosure, or sale of customer information without consent and service providers may not withhold service to a customer that does not consent.[115] Nevada's "Act relating to Internet privacy" requires Internet service providers to allow consumers to opt out of the sale of personal information to third parties.[116] Oregon's "Act [r]elating to actions with respect to a breach of security that involves personal information" requires covered entities, defined generally as an entity that collects or manages personal information, to notify customers and the Oregon attorney general in the event of a data breach.[117]

In March 2020, New York began enforcing the Stop Hacks and Improve Electronic Data Security (SHIELD) Act.[118] The law imposes an "affirmative duty on covered entities to implement reasonable data security to protect the private information of New York residents . . . ."[119] Zoom became one of the first targets of the SHIELD Act when the New York attorney general issued a consent decree that required Zoom to maintain stricter security standards and ensure compliance with the Act's mandates.[120] Zoom also "agreed to stop sharing user data with social media companies and to give videoconference hosts more control over outside access to videoconferences."[121]

In March 2021, Virginia became the second state behind California to enact comprehensive consumer privacy legislation.[122] The Virginia Consumer Data Protection Act (VCDP) "hands consumers the ability to access, correct and delete their personal information and to opt out of the processing of this data for targeted advertising purposes."[123] The legislation departs from the CCPA in several key respects, continuing the trend of inconsistent state privacy regulations. The VCDP adopted language and data assessment requirements more in line with the European Union's General Data Protection Regulation, and enforcement

115. An Act to Protect the Privacy of Online Customer Information, L.D. 946, 129th Leg. (Me. 2019).

116. An Act Relating to Internet Privacy, S.B. 220, 80th Leg. (Nev. 2019).

117. An Act Relating to Actions with Respect to a Breach of Security That Involves Personal Information, S.B. 684, 80th Leg. (Or. 2019).

118. An Act to Amend the General Business Law and the State Technology Law in Relation to Notification of a Security Breach, S.B. 5575B, 2019-2020 Reg. Sess. (N.Y. 2019).

119. Southwell et al., *supra* note 113 (internal quotations omitted).

120. *See Attorney General James Secures New Protections, Security Safeguards for All Zoom Users*, N.Y. ST. OFF. ATT'Y GEN. (May 7, 2020), http://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users.

121. Southwell et al., *supra* note 113.

122. *See* Consumer Data Protection Act, S.B. 1392, 2021 Gen. Assemb., 1st Spec. Sess. (Va. 2021) (to be codified at 59 Va. Admin. Code § 571-581).

123. Grande, *supra* note 101.

authority is vested exclusively in the state's attorney general, whereas the CCPA provides a limited private right of action.[124]

In April 2021, the Florida legislature considered comprehensive consumer privacy legislation, which would make it the third state to enact such a privacy framework.[125] The Florida House of Representatives overwhelmingly passed HB 969, moving it to the state Senate, which was also considering a narrower companion bill, SB 1734.[126] HB 969 is of particular interest to consumers and companies alike because it contains a private right of action allowing Florida residents "the right to access, delete and stop the sale of their personal information while allowing them to sue businesses that violate these provisions."[127] Technology trade groups oppose both bills, urging Florida legislators to consider the "disastrous effects that both ill-considered proposals could have on businesses and consumers."[128] The enactment of a privacy bill including a private right of action would be a huge step toward holding technology companies accountable for privacy violations, but Florida's new proposal is yet another strand in the complex web of American privacy laws.

C. The Complexity of Internet Privacy Law is Detrimental to Those Seeking Mental Health Treatment Online

Untangling the web of internet privacy law is a complicated task for the legally trained mind and entirely overwhelming for the average user. Understanding how federal and state privacy laws interact and staying up to date on current initiatives is an important yet often insurmountable task for those intent on sharing personal information on the internet. But those suffering from the negative mental health effects of the pandemic and those battling with substance abuse or other addiction must understand the risks associated with seeking remote treatment.

In addition to confusing laws, data breaches, and lawsuits against tech companies further erode trust in platforms like Zoom, Facebook, and Skype, pushing away more people seeking treatment. The next Part will

---

124. *See id.*

125. *See* Allison Grande, *Fla. Privacy Bill Would Be Compliance 'Disaster,' Group Says*, LAW360 (Apr. 26, 2021, 10:21 PM EDT), http://www.law360.com/articles/1378906/print?section=compliance.

126. An Act Relating to Consumer Data Privacy, H.B. 969, Reg. Sess. (Fla. 2021); An Act Relating to Consumer Data Privacy S.B. 1734, Reg. Sess. (Fla. 2021) (citing as the "Florida Privacy Protection Act").

127. Grande, *supra* note 125.

128. *Id.* (internal quotations omitted).

document some of the more prominent litigation surrounding data privacy and how these matters will impact the remote mental healthcare field.

IV. RELEVANT LITIGATION

The COVID-19 pandemic came on the tail of a record-breaking year of data breaches.[129] As life transitioned online, data breaches continued to increase in all industries including technology companies, hospitality, entertainment, healthcare, and even the federal government.[130] These breaches gave way to lawsuits, many ongoing, and several large settlements resolving older data breach cases. The increased scrutiny on companies' data security also led to lawsuits concerning unlawful policies and practices with regard to the exploitation of user data.

Particularly relevant to the practice of remote healthcare during the pandemic are a series of lawsuits brought against Zoom, which serve to highlight the platform's security vulnerabilities. In March 2020, a class action suit brought against Zoom alleged the unlawful sharing of user data with a social media partner in violation of the CCPA.[131] Rather than an actual data breach, the plaintiffs alleged the data sharing arrangement itself constituted a breach.[132] In April 2020, a class action lawsuit against Zoom accused the company of "misleading shareholders about the degree of its data privacy and security measures and failing to disclose that its service was not end-to-end encrypted."[133] Similarly, the suit does not allege actual data breach, but it does strengthen the position that Zoom is less secure than many would hope.[134]

In November 2020, Zoom entered into a cybersecurity settlement agreement with the FTC for allegedly unfair or deceptive trade practices.[135] The FTC alleged Zoom misrepresented the extent to which it

---

129. *Number of Records Exposed up 112% in Q3*, RISK-BASED SEC. (Nov. 12, 2019), http://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/ (indicating that 2019 was the "worst year on record" for data breaches).

130. *See, e.g.*, Christopher Bing, *Suspected Russian Hackers Spied on U.S. Treasury Emails—Sources*, REUTERS (Dec. 13, 2020), http://www.usnews.com/news/top-news/articles/2020-12-13/exclusive-us-treasury-breached-by-hackers-backed-by-foreign-government-sources.

131. *See* Compl. for Damages and Equitable Relief, Cullen v. Zoom Video Commc'ns, Inc., Litig., No. 5:20-cv-02155-SVK (N.D. Cal. Mar. 30, 2020).

132. *See* Southwell et al., *supra* note 113.

133. Drieu v. Zoom Video Commc'ns, Inc., Case No. 3:20-cv-02353-JP (N.D. Cal. Apr. 7, 2020); Kelly Zegers, *Shareholders Sue Zoom over Privacy, Hacking Concerns*, LAW360 (Apr. 8, 2020), http://www-law360-com.gwlaw.idm.oclc.org/articles/1261581/shareholders-sue-zoom-over-privacy-hacking-concerns.

134. *See generally* Zegers, *supra* note 133.

135. Zoom Video Commc'ns, Inc., No. 192-3167, 2020 WL 6589815 (F.T.C. Nov. 9, 2020).

encrypted video conferences and that Zoom committed deceptive and unfair practices with respect to its application for Apple Inc.'s computers.[136] Specifically, the FTC claimed "Zoom secretly installed software on Mac computers that introduced security vulnerabilities onto the devices."[137] Notably, the FTC did not allege any actual harm caused by the vulnerabilities.[138] In a nonmonetary data security settlement, the FTC prohibited Zoom from misrepresenting its privacy practices and required Zoom to "boost its data security practices."[139]

The settlement agreement drew sharp criticism from individuals, advocacy groups, and the two FTC Commissioners who voted to reject the agreement.[140] Commissioner Rebecca Kelly Slaughter wrote a dissenting statement, claiming the agreement should have "required Zoom to improve its privacy practices, not merely its security practices, as well as provide recourse for Zoom's paying customers."[141] Commissioner Rohit Chopra similarly argued for consumer recourse and discussed various ways in which he believes the FTC's enforcement in the privacy and cybersecurity space is ineffective.[142] However, other commentators claim the FTC overstepped its statutory authority to impose the additional security requirements.[143] Many companies are willing to accept settlement agreements with the FTC in order to avoid lengthy and costly litigation, which has allowed the FTC to impose penalties far exceeding its enforcement authority.[144]

Several other video conferencing and social media applications faced similar allegations during the past year.[145] Facebook paid $550 million to settle a facial recognition class action lawsuit stemming from Facebook's

136. *See FTC Requires Zoom to Enhance its Security Practices as Part of Settlement*, FED. TRADE COMM'N (Nov. 9, 2020), http://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement.

137. Doug Meal et al., *FTC Exceeded Its Authority in Zoom Cybersecurity Settlement*, LAW360 (Nov. 17, 2020, 6:15PM), http://www.law360.com/articles/1329620/print?section=appellate.

138. *See id.*

139. Allison Grande, *FTC Stands Behind Zoom Data Security Deal Despite Backlash*, LAW360 (Feb. 1, 2021, 10:49 PM), http://www.law360.com/articles/1350749/print?section=compliance.

140. *See generally* Meal et al., *supra* note 137.

141. *Id.*

142. *Id.*

143. *See id.*

144. *See id.*

145. *See, e.g.*, Class Action Compl. and Demand for Jury Trial, G.R. v. TikTok, Inc., No. 2:20-cv-04537 (C.D. Cal. May 20, 2020), ECF No. 1.

photo labeling service.[146] Illinois residents brought the class action against Facebook under a state law requiring "companies to obtain written permission before collecting a person's fingerprints, facial scans or other identifying biological characteristics."[147] The technology industry has argued in vain since the law's inception that claimants should be required to demonstrate actual harm, but courts denied Facebook's bid to have the suit dismissed.[148] Similarly, the social media company TikTok settled a class action suit accusing the company of "collecting users' biometric data without sufficient warning and using it to target content and ads on the app."[149] The Chinese-owned company denied the allegations, but agreed to a settlement in order to focus on improving their services.[150]

Amidst all the data privacy litigation, it comes as no surprise that many would hesitate to share important personal information, especially pertaining to mental health or addiction, on one of these platforms. Because most large-scale data privacy suits end in settlement, discerning their effectiveness at creating privacy policy is difficult.[151] In fact, because most data privacy actions involve settlement with the FTC, the content of those agreements has become the functional equivalent of a privacy common law.[152] While settlements have favored the FTC in its efforts to expand its enforcement authority over cybersecurity, settlements with individual consumers often favor the companies.[153]

---

146. *See In re* Facebook Biometric Information Privacy Litigation, 326 F.R.D. 535 (N.D. Cal. 2018); *see also* Natasha Singer & Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), http://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html.

147. Singer & Isaac, *supra* note 146.

148. *See id.*

149. Joe Walsh, *TikTok Settles Privacy Lawsuit for $92 Million*, FORBES (Feb. 25, 2021, 3:45 PM), http://www.forbes.com/sites/joewalsh/2021/02/25/tiktok-settles-privacy-lawsuit-for-92-million/?sh=3eac51a04872.

150. *See id.* (quoting TikTok spokesperson: "While we disagree with the assertions, rather than go through lengthy litigation, we'd like to focus our efforts on building a safe and joyful experience for the TikTok community,").

151. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585-87 (2014).

152. *See id.* at 586.

153. *See* Meal et al., *supra* note 137 (noting that settlement agreements have historically allowed big businesses to maintain opacity in operations); *see also* Michelle Conlin et al., *Special Report: Why Big Business Can Count on Courts to Keep Its Deadly Secrets*, REUTERS (Dec. 19, 2019, 6:13 AM), http://www.reuters.com/article/us-usa-courts-secrecy-lobbyist-specialre/special-report-why-big-business-can-count-on-courts-to-keep-its-deadly-secrets-idUSKBN1YN1GF.

V. MOVING FORWARD

The confusion surrounding data privacy laws and the vulnerability of many major technology platforms has created an environment where those in most need of help are uncomfortable seeking it. The methods of remote treatment that cropped up during the COVID-19 pandemic proved effective and are likely here to stay long after a return to normalcy. While there will always be a market for in-person therapy and support groups, the increase in access to mental healthcare is too beneficial to ignore.

Telehealth is one of many different areas impacted by privacy laws and, like all the others, would benefit greatly from a comprehensive federal data privacy scheme. Currently, the state patchwork system is insufficient to regulate internet service providers and establish robust security standards to protect user data. While the protections for personal health information under HIPAA are effective, they should be extended to other areas of healthcare including mental health treatment and support group programs. Perhaps once people seeking mental healthcare feel their personal information is secure, they will be open to the prospect of chatrooms, videoconferences, and online support groups.

Despite the confusion surrounding the various state privacy initiatives, the federal government would do well to take note of their success. California and, more recently, Virginia have established robust protections that will hopefully hold technology companies accountable and offer wary consumers some peace of mind. Florida seems to be next on the list, including potentially the most formidable consumer privacy right—the private right of action. Virulent opposition to Florida's legislation, led by big technology companies, suggests a considerable fear that consumers will take full advantage of the right to seek legal redress for privacy violations and inadequate cybersecurity.

Until a more applicable federal privacy framework is developed, companies offering remote mental healthcare applications should ensure patients and all those seeking treatment understand the potential privacy risks associated with engaging in such activities. Perhaps mental health professionals should be required to discuss these issues with patients engaged in remote treatment. Written disclaimers prior to beginning treatment may also be an effective solution. There is, of course, no single solution for such a complex issue, but framing future discussions with these concerns in mind may lead to more productive results. The opportunity to expand mental health treatment to people across the world in all socioeconomic situations is simply too important to squander.