Notre Dame Law Review

Volume 97 | Issue 1 Article 1

12-2021

Uncertain Terms

Leah R. Fowler
Research Assistant Professor, University of Houston Law Center, and Research Director, Health Law & Policy Institute

Jim Hawkins
Alumnae College Professor in Law, University of Houston Law Center

Jessica L. Roberts
Leonard H. Childs Chair in Law, Director of the Health Law & Policy Institute, Professor of Law, and Professor of Medicine (by courtesy), University of Houston

ARTICLES

UNCERTAIN TERMS

*Leah R. Fowler, Jim Hawkins & Jessica L. Roberts**

Health apps collect massive amounts of sensitive consumer data, including information about users' reproductive lives, mental health, and genetics. As a result, consumers in this industry may shop for privacy terms when they select a product. Yet our research reveals that many digital health tech companies reserve the right to unilaterally amend their terms of service and their privacy policies. This ability to make one-sided changes undermines the market for privacy, leaving users vulnerable. Unfortunately, the current law generally tolerates unilateral amendments, despite fairness and efficiency concerns. We therefore propose legislative, regulatory, and judicial solutions to better protect consumers of digital health tech and beyond.

* Fowler is Research Assistant Professor, University of Houston Law Center, and Research Director, Health Law & Policy Institute. This research was made possible by a New Faculty Research Grant from the University of Houston. Hawkins is Alumnae College Professor in Law, University of Houston Law Center. Roberts is Leonard H. Childs Chair in Law, Director of the Health Law & Policy Institute, Professor of Law, and Professor of Medicine (by courtesy), University of Houston. The authors thank the participants of the 2021 Rothenberg Health Care Law & Policy Virtual Speaker Series, 2020 Wiet Life Science Law Scholars Virtual Workshop, the 2020 Emory University School of Law Virtual Workshop on Vulnerability and Corporate Subjectivity, the 2020 AALS Health Law Virtual Workshop Series, and the University of Houston Faculty Works-in-Progress Series. We are especially grateful to Emily Berman, Dave Fagundes, Hank Greely, Diane Hoffmann, Nina Kohn, Craig Konnoth, Sapna Kumar, James Nelson, Anya Prince, D. Theodore Rave, Margaret Foster Riley, Alix Rogers, Karen Rothenberg, David Simon, Stacey Tovino, Charlotte Tschider, and Nina Varsava for their comments on earlier drafts. Taylor Hood, Farhan Mohiuddin, Jennifer Pier, and Jessie Totten provided excellent research assistance. Emily Lawson provided outstanding library support.

INTRODUCTION

In January 2021, the Federal Trade Commission (FTC) settled a complaint against the period- and fertility-tracking app Flo.[1] Flo, like many similar technologies in the booming digital health tech industry,[2] collects and analyzes its users' data to provide them with information and recommendations about their personal health.[3] To gain consumers' trust, Flo assured its users that it would keep their highly intimate data—information about menstruation, mood, sex drive, and pregnancy symptoms—safe, away from the prying eyes of third parties.[4] Yet an exposé in the *Wall Street Journal* revealed that the company had failed to keep its promises to consumers.[5] Flo was sharing its users' personal and identifiable data with numerous analytical and marketing firms without consumers' knowledge or consent. For example, Facebook received information that individual consumers were either having their periods or trying to get pregnant, allowing the social media platform to target its advertising to those users.[6] Consumers reported feeling "outraged," "victimized," and "violated."[7]

---

1 Flo Health, Inc., F.T.C. File No. 1923133 (Jan. 13, 2021) (agreement containing consent order) [hereinafter Flo Consent Order].

2 An estimated 52% of smartphone users already collect health information on their smartphones. Nehabaluni, *Mobile Medical Apps: A Game Changing Healthcare Innovation*, HEALTH WORKS COLLECTIVE, https://www.healthworkscollective.com/mobile-medical-apps-a-game-changing-healthcare-innovation/ [https://perma.cc/B3EJ-A3BD]. And over 325,000 healthcare apps are available for download. *Device Software Functions Including Mobile Medical Applications*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/digital-health-center-excellence/device-software-functions-including-mobile-medical-applications [https://perma.cc/RW8J-2G66] (last updated Nov. 5, 2019).

3 *See infra* Section I.A.

4 Lesley Fair, *Health App Broke Its Privacy Promises by Disclosing Intimate Details About Users*, FED. TRADE COMM'N (Jan. 13, 2021), https://www.ftc.gov/news-events/blogs/business-blog/2021/01/health-app-broke-its-privacy-promises-disclosing-intimate [https://perma.cc/A96B-LYZM].

5 Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 [https://perma.cc/UN54-KFZ7].

6 *Id.*

7 Fair, *supra* note 4.

It is well known that the average consumer will rarely read the terms of service (ToS) or privacy policies when selecting a product.[8] Conversely, in the context of digital health tech—where the data at stake is often sensitive—users may be more inclined to actually shop for privacy and to choose a product based on a company's purported terms. Health app providers spend significant advertising dollars on proclaiming their products' commitments to privacy and data security to attract consumers.[9] These advertisements create a market for privacy in digital health tech, with users selecting apps based at least in part on the companies' promises regarding privacy and data security. The potential reliance on a company's privacy terms made Flo's transgression even more troubling. As one commentator on the recent controversy explained: "It's become even more cynical than just 'buyer beware'. . . . You did your homework. You read this app's privacy policy. You thought you were putting your data in a trusted place. And turns out that the company didn't take its obligation seriously."[10] The point is simple: if companies don't keep their promises, the data of even informed, responsible users will not be safe.

The FTC's responsibilities include policing "unfair and deceptive acts or practices" that harm consumers.[11] It filed a complaint against Flo because of the company's repeated deceptive statements to its users about their privacy.[12] As noted, Flo ultimately settled with the FTC.[13] As part of the settlement, the company agreed to a review of its privacy practices and vowed to obtain users' consent before sharing their data in the future.[14] The FTC had jurisdiction over Flo's actions because the company had effectively *lied* to its users. It said one thing and did another. But what if a health app could go back on its promises to consumers without violating its ToS or privacy policies?

Remarkably, Flo could have done just that. If the company had simply changed its ToS or privacy policy, it could have shared its customers' data without lying to them at all. Flo is one of the many companies that include unilateral amendment clauses in their

---

8 *See infra* notes 84–87 and accompanying text.

9 *See infra* subsection I.B.2.

10 Alisha Haridasani Gupta & Natasha Singer, *Your App Knows You Got Your Period. Guess Who It Told?*, N.Y. TIMES (Jan. 28, 2021), https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html [https://perma.cc/WZ8J-ZKZ6].

11 *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/ZTW3-JFU2]; *see also A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N [hereinafter *Overview of FTC's Authority*], https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/9B8E-GHRD] (last updated May 2021).

12 *See* Fair, *supra* note 4.

13 Flo Consent Order, *supra* note 1.

14 *Id.*

agreements with consumers.[15] Under these provisions, companies can alter terms sometimes without even notifying users, let alone asking them for permission. And unilateral amendments are by and large legal. More often than not, courts are willing to enforce these one-sided changes.[16] If Flo had simply changed its terms, the company might have been able to avoid running afoul of the FTC's prohibitions on deceptive trade practices.[17] In fact, consumers currently have very little legal recourse for challenging harmful unilateral amendments. The result is that even users who actively read ToS and privacy policies when selecting a product remain vulnerable to changes that happen without their knowledge and could compromise their privacy. Thus, unilateral amendment clauses undermine the market for privacy that exists in digital health tech.[18]

Scholars have long argued that one-sided changes to contract terms are both inefficient and unfair.[19] While unilateral amendment provisions may be problematic in a variety of contexts,[20] we maintain that they are especially troubling in the context of health apps. Flo is hardly alone in reserving the right to unilaterally amend its agreements. For this Article, we surveyed the ToS and privacy policies of thirty digital health tech companies. Nearly all of the companies reserved the right to change their ToS, and all of the companies reserved the right to change their privacy policies.[21] While most apps promised to at least notify users when modifications occurred, some put the responsibility of staying up to date on the individual consumers themselves.[22] And, because courts enforce unilateral amendments, the only choice for a savvy user who wishes to challenge a harmful unilateral amendment is to stop using the product. In the context of health apps, terminating use may mean abandoning weeks, months, or even years of potentially valuable personal data. Given the high stakes of digital health tech, consumers need stronger legal protections against potentially harmful one-sided changes.

This Article focuses exclusively on direct-to-consumer health apps. However, what we describe here provides only a snapshot of a much

15 *See infra* Section I.C.

16 *See infra* Section II.A.

17 Of course, the company would also have had to change its advertising strategy to avoid misleading consumers. For a more detailed discussion of the FTC's regulatory authority, *see infra* subsection II.A.3.

18 *See infra* subsection I B.2.

19 *See infra* subsection II.B.1.

20 *E.g.*, David A. Hoffman & Tess Wilkinson-Ryan, *The Psychology of Contract Precautions*, 80 U. CHI. L. REV. 395, 398–99 (2013); David Horton, *The Shadow Terms: Contract Procedure and Unilateral Amendments*, 57 UCLA L. REV. 605, 606 (2010).

21 *See infra* Section I.C, Table 1; *see also infra* Appendix.

22 *See infra* Section I.C, Tables 2 & 3.

larger problem. In addition to buying products on the consumer market, individuals may also download health apps through their healthcare providers and their employers. These technologies have their own separate regulatory structures and raise their own unique sets of legal concerns.[23] Moreover, the issues that we identify are not confined to digital health tech. Consumers of other technologies are likewise at risk. Navigation apps, budgeting apps, and dating apps all collect sensitive, identifiable, personal data that many users would prefer to keep private.[24] Thus, while our focus is direct-to-consumer health apps, the legislative, regulatory, and judicial solutions that we propose could benefit other kinds of users subject to unwanted one-sided changes.

This Article proceeds in three parts. Part I offers an introduction to health apps and argues that the proliferation of unilateral amendment clauses in that industry leads to market failures. Part II then turns to the current law governing one-sided changes and the critiques of unilateral amendment provisions, both generally and in the context of digital health tech. We also note the limited benefits of one-sided changes. In Part III, we discuss legislative, regulatory, and judicial innovations to better protect all consumers, not just the users of digital health tech. We focus on how these various kinds of interventions can give companies the flexibility that they need while ensuring that consumers have the legal protections that they deserve.

I. PROTECTING PRIVACY IN DIGITAL HEALTH TECH

Privacy may be of particular concern to users of digital health tech. Part I begins with a brief introduction to health apps, identifies the privacy issues that they may raise, and explores their potential benefits for consumers. We then turn to our original research assessing the advertising, ToS, and privacy policies of thirty health apps. We conclude that health app consumers may choose a particular service based on a company's promises to protect user data. Despite this reliance by consumers, almost every health app that we surveyed

23 For example, in addition to its direct-to-consumer services, Ovia provides fertility and pregnancy counseling services for employees, including return-to-work programming. *No Two Families Are the Same – Why Should Their Care Be?*, OVIA HEALTH, https://www.oviahealth.com/employer-family-benefits/ [https://perma.cc/2VQE-6BDS]. The company sold information about users' "ovulation cycles, medications, [and] pregnancy," among other things, to users' employers through employer-sponsored wellness programs. Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 N.Y.U. L. REV. 662, 664 (2019). Employers could potentially use those data to discriminate. Stephanie R. Morain, Leah R. Fowler & Jessica L. Roberts, *What to Expect When [Your Employer Suspects] You're Expecting*, JAMA INTERNAL MED. 1597, 1597–98 (2016).

24 *See infra* notes 261–63 and accompanying text.

reserves the right to change their ToS and privacy policy without consent and—in some cases—without clear notice. We assert that this potential for one-sided changes distorts the market for privacy in digital health tech, leaving consumers of health apps and their most private data vulnerable.

A. Health Apps

Health apps collect and warehouse large amounts of highly sensitive user data. Consumers of digital health tech therefore have a strong interest in wanting to keep that information private. Despite the potential privacy risks, these technologies offer serious benefits for users, especially in the context of the United States' fragmented healthcare system. This Section introduces three different categories of health apps, considers their accompanying privacy concerns, and assesses their potential benefits.

1. Examples of Health Apps

One needs to look no further than the "Health & Fitness" section of the Apple App Store to appreciate the enormous—and lucrative—market for health apps.[25] Despite their diversity, almost all of these technologies collect and store intimate personal information about their users, information that consumers would likely prefer to remain private.[26] Here, we describe three distinct categories of digital health technology—(1) femtech apps; (2) mental health apps; and (3)

25 Jennifer K. Wagner, *The Federal Trade Commission and Consumer Protections for Mobile Health Apps*, 48 J.L. MED. & ETHICS (SPECIAL SUPP. 48:1) 103, 103 (2020) ("[P]rojections for the global mHealth app market—of which North American is considered the leading region and the U.S. is the leading country within that region—are that it will generate more than $111 Billion U.S. dollars by 2025."). They can be used to "track, monitor and act on," among others, "physiological, psychological or social health data." Katie Gambier-Ross, David J. McLernon & Heather M. Morgan, *A Mixed Methods Exploratory Study of Women's Relationships with and Uses of Fertility Tracking Apps*, 4 DIGIT. HEALTH 1, 1–2 (2018). They can also sync with wearable devices to gather additional data and provide users with more customizable feedback. John P. Higgins, *Smartphone Applications for Patients' Health and Fitness*, 129 AM. J. MEDICINE 11, 13 (2016). Some wearables are as visible as the Fitbit and Apple watches we see on wrists every day. Other sensors are more private and hidden, such as the intravaginal sensors that can sync with smartphones to provide core body temperature measurements or reports on Kegel exercises. *See, e.g.*, *Strengthen Your Pelvic Floor with Games*, PERIFIT, https://perifit.co/ [https://perma.cc/XKM3-WJ43] (Perifit Sensor and App); *Why Guess When You Can Know?*, PRIYA, https://www.kindara.com/products/priya-fertility-monitor/ [https://perma.cc/EAM9-LVFB] (Priya Sensor and App).

26 Violations of consumer privacy can happen in at least one of two ways. One, the company could have an insecure platform that is vulnerable to hacking. Two, the company could voluntarily share its users' data, often for a profit.

genetics apps—and their privacy implications. We selected these particular health apps because each of the three categories implicates a different type of highly sensitive health-related data.

a. Femtech Apps

"Femtech" apps provide a wide range of gynecological and obstetric services. These technologies perform a variety of functions, such as tracking menstruation, predicting fertility, assisting natural family planning, and sending digital reminders to take hormonal birth control pills.[27] While most of the marketing in this industry targets millennials,[28] younger consumers may use apps to log their periods[29] and older consumers may download them to monitor their menopause symptoms.[30] Femtech apps can then analyze data collected from consumers to generate reports with information and predictions about a user's current or future health status.[31] The user may then use those reports to make reproductive or other health-related decisions.

To perform their functions, many femtech apps house, store, and analyze large amounts of deeply personal information. These data include a variety of potentially sensitive details about users' lives, including the characteristics of their vaginal discharge, the level of their libidos, and the details of their sexual encounters.[32] Consumers might want to keep this information private for a variety of reasons. To start, the nature of the data itself is highly intimate. Many people would prefer that third parties did not know how often they have sex or whether they are trying to conceive.[33] For younger users, their data

27 Ida Tin, *The Rise of a New Category: Femtech*, CLUE (Sept. 14, 2016), https://helloclue.com/articles/culture/rise-new-category-femtech [https://perma.cc/6JSZ-RC5T]. For example, apps like Clue and Flo use user data to generate predictions about menstruation and ovulation. CLUE, https://helloclue.com [https://perma.cc/77J8-59F8]; FLO, https://flo.health/ [https://perma.cc/W338-TE5A].

28 ReportLinker, *Global Female Technology (Femtech) Market: Analysis and Forecast, 2019-2030*, GLOBENEWSWIRE (June 10, 2020), https://www.globenewswire.com/news-release/2020/06/10/2046213/0/en/Global-Female-Technology-Femtech-Market-Analysis-and-Forecast-2019-2030.html [https://perma.cc/59K6-6VNL].

29 Leah R. Fowler, Charlotte Gillard & Stephanie Morain, *Teenage Use of Smartphone Applications for Menstrual Cycle Tracking*, PEDIATRICS, May 2020, at 1, 1.

30 Elise Mortensen, *Menopause: The DTC Digital Health Up-and-Comer*, HTD HEALTH (July 21, 2020), https://htdhealth.com/insights/menopause-the-dtc-digital-health-up-and-comer/ [https://perma.cc/MJ52-744Z].

31 Celia Rosas, Note, *The Future is Femtech: Privacy and Data Security Surrounding Femtech Applications*, 15 HASTINGS BUS. L.J., 319, 320–322 (2019).

32 *See* Karen E.C. Levy, *Intimate Surveillance*, 51 IDAHO L. REV. 679, 684 (2015).

33 For example, when to announce a pregnancy can be a very important decision for many people. *See* Holly Pevzner, *When Is it Safe to Announce Your Pregnancy?*, TODAY'S PARENT (Dec. 14, 2018), https://www.todaysparent.com/pregnancy/when-is-it-safe-to-announce-pregnancy/ [https://perma.cc/LH9W-QRCG].

might become a source of gossip or bullying.[34] Moreover, consumers who are survivors of intimate partner violence might fear that these private details could end up in the hands of their abusers.[35] The leaking or sharing of femtech data without user consent could result in a variety of potential privacy violations, ranging from dignitary harms like embarrassment to more tangible injuries like stalking and discrimination. Despite their susceptibility to hacking,[36] some consumers ironically use femtech apps because they perceive those technologies to be *more private* than traditional paper tracking methods.[37]

b. Mental Health Apps

Mental health apps can also take a variety of forms.[38] Some attempt to replicate a traditional provider-patient interaction.[39] Others use large datasets to simulate the therapeutic relationship using "chatbots."[40] Mental health apps may also take a less conventional approach. Instead of modeling traditional therapeutic relationships,

34 Fowler et al., *supra* note 29, at 2.

35 In fact, one of the apps in our study, Glow, was once dubbed "a [j]ackpot for [s]talkers." Kelly Weill, *This Fertility App is a Jackpot for Stalkers*, DAILY BEAST, https://www.thedailybeast.com/this-fertility-app-is-a-jackpot-for-stalkers [https://perma.cc/X2GR-62HA] (Apr. 13, 2017). The company has since stepped up its data security measures. Kaitlyn Tiffany, *Period-Tracking Apps Are Not for Women*, VOX (Nov. 16, 2018), https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health [https://perma.cc/Q6KA-VZDS].

36 Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REPS. (Sept. 17, 2020), https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/ [https://perma.cc/FMT2-8UG5]; COOPER QUINTIN, ELEC. FRONTIER FOUND., THE PREGNANCY PANOPTICON 3 (2017).

37 Daniel A. Epstein et al., *Examining Menstrual Tracking to Inform the Design of Personal Informatics Tools*, *in* ASS'N FOR COMPUTING MACH. SPECIAL INT. GRP. ON COMPUT.-HUM. INTERACTION, CHI '17: PROCEEDINGS OF THE 2017 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 6876, 6883 (2017) (stating that "[s]ome women prefer using a dedicated app because of privacy, including S192: '*keeping info in an app instead of written on my calendar gives me greater privacy*'"); *see also* Amanda Karlsson, *A Room of One's Own? Using Period Trackers to Escape Menstrual Stigma*, NORDICOM REV., June 2019, at 111, 111.

38 ONE MIND PSYBERGUIDE, https://onemindpsyberguide.org/ [https://perma.cc/94T5-CHHK].

39 TALKSPACE, https://www.talkspace.com/ [https://perma.cc/9YTJ-SV9W]. For example, TalkSpace matches consumers with a licensed therapist. *Id.*

40 Michael Mattioli, *Pooling Mental Health Data with Chatbots*, *in* GOVERNING PRIVACY IN KNOWLEDGE COMMONS 70, 70 (Madelyn Rose Sanfilippo, Brett M. Frischmann & Katherine J. Strandburg eds., 2021); WOEBOT HEALTH, https://woebot.io/ [https://perma.cc/Q49G-T6DT].

these apps can also support mindfulness exercises,[41] self-diagnosis,[42] and "brain training" activities based on cognitive-behavioral principles.[43] Interestingly, users of mental health apps appear to skew young[44] and female.[45]

Like femtech apps, mental health apps must collect sensitive consumer data. For example, a user may answer questions about feelings of self-worth, subjective mental state, and even suicidal ideation.[46] Mental health apps then use this information to tailor their services and recommendations. Again, users may very well want to keep this information private. Unfortunately, mental health stigma remains high in the United States.[47] People who could benefit from treatment may avoid seeking help because they fear being labeled mentally ill and facing the associated stereotypes and discrimination.[48] Mental health apps might provide an alternative for consumers who want to avoid the potential stigma of diagnosis. Research suggests users may be more candid when interacting with technology than with other humans.[49] Yet for the very same reasons that these users decline traditional mental healthcare, they will want to keep their mental health app data private. Not only could that information, if

41 HEADSPACE, https://www.headspace.com/headspace-meditation-app [https://perma.cc/7XRU-8UMM].

42 *Wellness*, MINDMATTERS, https://www.mind-matters.co/projects/wellness [https://perma.cc/6ES5-WP73].

43 *See* REMENTE, https://www.remente.com/ [https://perma.cc/PES5-JYVX] (last visited Sept. 24, 2021).

44 John Torous, Hannah Wisniewski, Gang Liu & Matcheri Keschavan, *Mental Health Mobile Phone App Usage, Concerns, and Benefits Among Psychiatric Outpatients: Comparative Survey Study*, J. MED. INTERNET RSCH. MENTAL HEALTH, Oct.–Dec. 2018, at 1, 8.

45 Rachel Smail-Crevier, Gabrielle Powers, Chelsea Noel & JianLi Wang, *Health-Related Internet Usage and Design Feature Preference for E-Mental Health Programs Among Men and Women*, J. MED. INTERNET RSCH., Mar. 2019, at 1, 8.

46 For example, Depression Test, by MindMatters, asks the user about standard diagnostic criteria for depression, including desires for self-harm. *See Wellness*, *supra* note 42. MindDoc inquires about feelings of worthlessness. *MindDoc*, MOODPATH, https://mymoodpath.com/en/ [https://perma.cc/J46C-2AJU/]. Others, like What's Up, allow for free-text entry about how a user feels, positive and negative habits, and general notes. *What's Up?—A Mental Health App*, APPLE, https://apps.apple.com/us/app/whats-up-a-mental-health-app/id968251160 [https://perma.cc/Z3UT-HY48].

47 Angela M. Parcesepe & Leopoldo J. Cabassa, *Public Stigma of Mental Illness in the United States: A Systematic Literature Review*, 40 ADMIN. & POL'Y IN MENTAL HEALTH & MENTAL HEALTH SERVS. RSCH. 384, 384 (2013).

48 Patrick W. Corrigan, Benjamin G. Druss & Deborah A. Perlick, *The Impact of Mental Illness Stigma on Seeking and Participating in Mental Health Care*, 15 PSYCH. SCI. PUB. INT. 37, 37 (2014).

49 Gale M. Lucas, Jonathan Gratch, Aisha King & Louis-Philippe Morency, *It's Only a Computer: Virtual Humans Increase Willingness to Disclose*, 37 COMPUTS. HUM. BEHAV. 94, 98 (2014).

compromised, cause shame or embarrassment, but it could also lead to discrimination in employment, housing, healthcare, or other areas.[50]

c. Genetics Apps

Lastly, genetic apps collect and warehouse their users' genetic information. Like the other two categories, they provide a range of products and services. Some companies require users to purchase a test kit, collect their DNA (usually in the form of a cheek swab or a vial of spit), and mail the sample off for analysis.[51] Other companies act primarily as data repositories where consumers upload their existing genetic data for storage on the platform and to use that company's specific services.[52] Unlike the previous two categories of apps, consumers of these technologies tend to be older.[53]

Genetics can reveal all kinds of intimate details about our lives, including our genetic relatives, our ancestry, and our health risks. For example, some companies offer genetic genealogy services designed to connect consumers with long-lost family members.[54] Others provide users with information about their personal health risk,[55] give consumers an opportunity to participate in genetic research,[56] or—sometimes quite dubiously—generate recommendations for improving health based on personal genetics through diet and lifestyle modifications.[57] Moreover, as the examples of FamilyTreeDNA and GEDmatch described below demonstrate, law enforcement may use

50 As a result of mental health stigma, once a person is labeled mentally ill, "employers may not want to hire them, landlords may not want to rent to them, or primary care doctors may provide substandard care." Corrigan et al., *supra* note 48, at 51.

51 *How It Works*, 23ANDME, https://www.23andme.com/howitworks/ [https://perma.cc/ZD9W-AEH8]; *Know Your World from the Inside*, ANCESTRY, https://www.ancestry.com/dna/ [https://perma.cc/Y47K-K8SN].

52 MYGENOMEBOX, https://www.mygenomebox.com [https://perma.cc/6EFG-RGXA]; DNA ID, https://www.dnaid.co/ [https://perma.cc/PDL7-HJEU].

53 Nikki M. Carroll et al., *Demographic Differences in the Utilization of Clinical and Direct-to-Consumer Genetic Testing*, 29 J. GENETIC COUNSELING 634, 638 (2020).

54 23ANDME, https://www.23andme.com [https://perma.cc/9AJX-QENW]; ANCESTRY, https://www.ancestry.com [https://perma.cc/TCL9-UH53]; DNA2TREE, https://www.dna2tree.com/ [https://perma.cc/7JDP-8QK5].

55 23ANDME, *supra* note 54; *Know Your World from the Inside*, *supra* note 51.

56 ALL OF US, https://www.joinallofus.org/ [https://perma.cc/296N-UUVY]; DNA ID, *supra* note 52.

57 MyGenomeBox encourages users to "[h]ave [f]un [w]ith [y]our DNA" and to "[c]ustomize your lifestyle based on what your DNA tells you!" MYGENOMEBOX, *supra* note 52 (click "How to Use Our Services"). Genetica offers data-driven and scientific reports that help you design the optimal lifestyle for you and your family. GENETICA, https://www.genetica.asia [https://perma.cc/55MV-3PC4].

consumer genetic databases to solve crimes.[58] Like with the information collected by femtech and mental health apps, genetic data could lead to privacy harms. People may feel violated simply because a company shared their genetic information without consent.[59] While the Genetic Information Nondiscrimination Act prevents employers and health insurers from discriminating on the basis of genetic data,[60] a whole host of potential discriminators—including schools, lenders, and other insurers—can lawfully make decisions based on someone's genetic information. Thus, users of genetics apps also have a strong interest in maintaining the privacy of their data.

2. Benefits of Health Apps

Despite these understandable privacy concerns, digital health tech offers services that consumers value.[61] Health apps have significant upsides for consumers, including providing users with potentially actionable health-related information when other health care services may be unavailable and allowing users to take a more proactive role in managing their own health. We consider each of these benefits in turn.

First, health apps may give people access to important health-related information and services they may otherwise lack. American health care is notoriously expensive and difficult to access.[62] A variety of populations experience health disparities as a result, including people of color,[63] people with disabilities,[64] and the poor.[65] While many Americans still cannot access adequate health care, the vast majority of adults own a smartphone.[66] Because these numbers hold

58 *See* discussion *infra* subsection I.B.2.

59 Cole v. Gene by Gene, Ltd., No. 14-CV-0004, 2017 WL 2838256, at *2–3 (D. Alaska June 30, 2017). In this case, the plaintiff did not suffer any physical or financial harm as a result of the alleged privacy violation.

60 42 U.S.C. §§ 300gg-53, 2000ff-1.

61 That value is part of the reason the thriving market for health apps is projected to be worth over $111 billion by 2025. Wagner, *supra* note 25, at 103.

62 Irene Papanicolas, Liana R. Woskie & Ashish K. Jha, *Health Care Spending in the United States and Other High-Income Countries*, 319 JAMA 1024, 1025 (2018).

63 NAT'L ACADS. OF SCIS., ENG'G & MED., COMMUNITIES IN ACTION: PATHWAYS TO HEALTH EQUITY 58–60 (James N. Weinstein, Amy Geller, Yamrot Negussie & Alina Baciu eds., 2017).

64 *Id.* at 75–76.

65 Dave A. Chokshi, *Income, Poverty, and Health Inequality*, 319 JAMA F.1312, 1312 (2018).

66 In 2021, 85% of adults owned a smartphone. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/YTJ7-BT2G]. This number exceeds percentage ownership of desktop and laptop computers (77%), tablet computers (53%), and e-readers (22% in 2016). *Id.*

relatively constant across demographic sectors,[67] research shows that mobile technology may be a promising method for reaching underserved populations.[68] Health apps, therefore, hold immense potential, particularly for populations with health disparities.[69] By bringing these health resources directly to anyone with a smartphone, health apps have the potential to reduce inequality and inequity, address challenges with health care accessibility, and ultimately improve health for all.[70]

Each category of digital health tech discussed above may offer an accessible and affordable alternative to traditional health care. Femtech apps can perform functions that previously required an appointment with a doctor, midwife, or doula, like fetal heart rate monitoring,[71] alternatives to hormonal birth control,[72] or pelvic floor therapy.[73] They also give teens and young adults direct access to information to help them understand their developing bodies.[74] Given the inconsistent legislative support for sexual education, these apps could serve as sources of information on sexual and reproductive health.[75] In the context of mental health, digital health tech can eliminate many well-documented barriers to treatment. Beyond the

67 *Id.*

68 Stephanie J. Mitchell, Leandra Godoy, Kanya Shabazz & Ivor B. Horn, *Internet and Mobile Technology Use Among Urban African American Parents: Survey Study of a Clinical Population*, J. MED. INTERNET RSCH., Jan. 2014, at 1, 1.

69 Maged N. Kamel Boulos, Steve Wheeler, Carlos Tavares & Ray Jones, *How Smartphones Are Changing the Face of Mobile and Participatory Healthcare: An Overview, with Example from eCAALYX*, 10 BIOMEDICAL ENG'G ONLINE, no. 24, 2011, at 1, 3–4.

70 That is not to say that relying on technology for modern health resources would not be a barrier for those without access. The most significant differences in access to smartphones were in populations over the age of sixty-five and those without a high school education. Despite this disparity, the majority of these groups—61% of Americans sixty-five or older and 75% of those with a high school education or less—still had access to a smartphone. *See Mobile Fact Sheet*, *supra* note 66.

71 Though not included in the present study, one example of a fetal heart rate monitoring app is: *My Baby Heart Rate Recorder*, APPLE, https://apps.apple.com/us/app/my-baby-heart-rate-record-er-heartbeat-listen-er/id1180751395 [https://perma.cc/69TY-M9GB].

72 For example, *Natural Cycles* markets itself as the "first FDA cleared birth control app," which can take the place of a prescription for hormonal contraception. NAT. CYCLES, https://www.naturalcycles.com/ [https://perma.cc/P5R4-N2XU].

73 *Strengthen Your Pelvic Floor with Games*, *supra* note 25.

74 ELLEN WARTELLA, VICKY RIDEOUT, HEATHER ZUPANCIC, LEANNE BEAUDOIN-RYAN & ALEXIS LAURICELLA, NW. UNIV., TEENS, HEALTH, AND TECHNOLOGY: A NATIONAL SURVEY 23 (2015) (observing that period tracking apps are the second most popular health-related mobile apps among girls ages 13–18); *see also* Fowler et al., *supra* note 29.

75 Lynae M. Brayboy, Alexandra Sepolen, Taylor Mezoian, Lucy Schultz, Benedict S. Landgren-Mills, Noelle Spencer, Carol Wheeler & Melissa A. Clark, *Girl Talk: A Smartphone Application to Teach Sexual Health Education to Adolescent Girls*, 30 J. PEDIATRIC & ADOLESCENT GYNECOLOGY 23, 23–24 (2017).

stigma discussed above, Americans face serious barriers to accessing mental health services, including high costs and inadequate insurance coverage,[76] limited options and long wait times,[77] and logistical challenges like finding reliable transportation.[78] And finally, genetic apps give consumers direct access to genetic information, something that would have previously required going to a physician or a genetic counselor. Like with femtech apps and mental health apps, these technologies offer lower cost and more convenient alternatives to conventional health care.

Second, health apps allow users to take a more proactive role in the management of their health. As explained above, digital health tech removes physician intermediaries. Because research shows that users may be more candid when interacting with technology than with other humans,[79] health app data may, in fact, be more accurate than traditional medical records. Moreover, the near-constant and long-term nature of the data collection means that health apps collect more—and sometimes better—patient-specific information than can be obtained in short and infrequent medical encounters.[80] As a result, digital health tech, used in conjunction with fitness wearables and artificial intelligence, shows great promise to support medical decision making.[81] Thus, even for users who have ready access to affordable health care, health apps can offer important upsides.

Under the current circumstances, users of health apps may have to sacrifice their privacy to obtain the benefits of these technologies.

B. Market for Privacy in Digital Health Tech

As a general matter, Americans value privacy.[82] Whether this affinity affects their consumer choices is a matter of significant debate in contract law and theory.[83] Evidence suggests that the vast majority

---

76 Kathleen Rowan, Donna D. McAlpine & Lynn A. Blewett, *Access and Cost Barriers to Mental Health Care, by Insurance Status, 1999-2010*, 32 HEALTH AFFS. 1723, 1728–1729 (2013).

77 Paul Wood, Joy Burwell & Kaitlyn Rawlett, *New Study Reveals Lack of Access as Root Cause for Mental Health Crisis in America*, NAT'L COUNCIL FOR MENTAL WELLBEING (Oct. 10, 2018), https://www.thenationalcouncil.org/press-releases/new-study-reveals-lack-of-access-as-root-cause-for-mental-health-crisis-in-america/ [https://perma.cc/PWG6-RZPX].

78 R. Mojtabai et al., *Barriers to Mental Health Treatment: Results from the National Comorbidity Survey Replication*, 41 PSYCH. MED. 1751, 1752–54 (2011).

79 Lucas et al., *supra* note 49, at 98.

80 Nathan G. Cortez, I. Glenn Cohen & Aaron S. Kesselheim, *FDA Regulation of Mobile Health Technologies*, 371 NEW ENG. J. MED. 372, 372–73 (2014).

81 Ida Sim, *Mobile Devices and Health*, 381 NEW ENG. J. MED. 956, 956 (2019).

82 *See* JEFFREY PRINCE & SCOTT WALLSTEN, TECH. POL'Y INST., HOW MUCH IS PRIVACY WORTH AROUND THE WORLD AND ACROSS PLATFORMS 2–3 (2020).

83 *See, e.g.*, Uri Benoliel & Shmuel I. Becher, *The Duty to Read the Unreadable*, 60 B.C. L. REV. 2255 (2019); Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract*

of consumers do not read terms[84] and instead rely on social norms and personal experiences to understand their relationships with companies.[85] In spite of these realities, some law and economics scholars have argued that consumers may still have some influence, pursuant to the informed minority hypothesis. According to this reasoning, even if only a minority of users select products based on terms, companies will compete for those buyers by offering favorable provisions.[86] Particularly relevant to this Article, some have even argued that companies will avoid unilateral amendment provisions to attract this savvy subset of customers.[87]

The informed minority hypothesis has faced criticism in light of evidence that no one—not even the most discerning user—actually reads the fine print.[88] However, if that theory has any traction, it would most likely be here. Unlike other markets, health apps collect data that are particularly intimate, and, as discussed below, there is good reason to believe that users may actually care about ToS and privacy policies more than the average consumer.

Law, 66 STAN. L. REV. 545 (2014); Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts"*, 78 U. CHI. L. REV. 165, 179–81 (2011); Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 649 (2011); Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429 (2002); *see also* Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1174 (1983); Arthur Allen Leff, *Unconscionability and the Code—The Emperor's New Clause*, 115 U. PA. L. REV. 485 (1967); Friedrich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943).

84 Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 1 (2014) (testing the informed-minority hypothesis by studying "the Internet browsing behavior of 48,154 monthly visitors to the Web sites of 90 online software companies to study the extent to which potential buyers access the end-user license agreement" and finding that "only one or two of every 1,000 retail software shoppers access the license agreement and that most of those who do access it read no more than a small portion"); *see also* Marotta-Wurgler, *supra* note 83, at 173.

85 Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. (SUPP.) S69, S87 (2016).

86 Yonathan A. Arbel & Roy Shapira, *Consumer Activism: From the Informed Minority to the Crusading Minority*, 69 DEPAUL L. REV. 233, 234 (2020).

87 *See* Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630 (1979) (arguing based on economic reasoning that companies will not put one-sided terms into contracts in order to attract those customers who read the contracts).

88 Arbel & Shapira, *supra* note 86, at 234.

1. Advertisements as Proxies for Consumer Preferences

Unlike the general population, users of digital health tech may actually shop for privacy terms when selecting a product. Because many Americans do not trust tech companies,[89] health app providers must win consumer trust before a person is willing to use their products. Moreover, featuring privacy protections can be lucrative. Research shows that when companies advertise their privacy policies prominently, consumers will pay a premium for greater protections.[90]

Thus, the best indicator that health app users select products based on their privacy provisions is that digital tech companies market those terms. Companies devote significant resources to advertising.[91] Because advertisers study what attracts consumers to certain products,[92] a company's marketing materials provide a window into what it thinks its consumers value.[93] Quite tellingly, many of the health app providers that we studied tout their commitment to privacy to attract users. In particular, digital health tech companies promote the rights of their consumers to control access to sensitive information. Health apps in each category that we surveyed promised consumers that their data would remain both private and secure.

Femtech websites acknowledge the intimate nature of the information they collect and vow not to sell or share consumers' data. For example, Flo promises users: "Your personal data security is our top priority at Flo. We do understand that your app profile may contain highly sensitive personal data. Therefore, every day we do our best to implement industry best practices and standards."[94] Glow similarly assured customers that it:

---

89 In a recent survey, 45% of respondents reported doubt that the technology sector protects customer data well, and 51% doubted that tech values consumer welfare more than profits. EDELMAN, 2019 EDELMAN TRUST BAROMETER: TRUST IN TECHNOLOGY 9 (2019).

90 Janice Y. Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RSCH. 254, 254 (2011) ("When such information is made available, consumers tend to purchase from online retailers who better protect their privacy. In fact, our study indicates that when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.").

91 Kyle Bagwell, *The Economic Analysis of Advertising*, *in* 3 HANDBOOK OF INDUSTRIAL ORGANIZATION 1701, 1704 (Mark Armstrong & Rob Porter eds., 2007).

92 Sarah C. Haan, Note, *The "Persuasion Route" of the Law: Advertising and Legal Persuasion*, 100 COLUM. L. REV. 1281, 1282 (2000).

93 For a series of articles exploring and justifying this claim, see Jim Hawkins & Renee Knake, *The Behavioral Economics of Lawyer Advertising: An Empirical Assessment*, 2019 U. ILL. L. REV. 1005; Jim Hawkins, *Exploiting Advertising*, 80 LAW & CONTEMP. PROBS. 43 (2017); Jim Hawkins, *Using Advertisements to Diagnose Behavioral Market Failure in the Payday Lending Market*, 51 WAKE FOREST L. REV. 57 (2016).

94 *Security*, FLO, https://flo.health/security [https://perma.cc/DZH4-Y9HH].

> [T]akes issues of privacy and the protection not only of personal health information, but all kinds of information about your private life very seriously. As discussed below we take great efforts to protect your information from disclosure, to use your information only to provide services to you, to improve the service for you, to improve our ability to provide services to other people in a similar situation, and to assist researchers in finding better ways to improve health.[95]

The website practically screams at consumers that the company will not share data without user consent: "WE DO NOT SELL OR RENT YOUR PERSONAL DATA TO THIRD PARTIES. WE DON'T SHARE YOUR INFORMATION (OTHER THAN FORUM POSTS) TO SOCIAL NETWORKS OR OTHER PUBLIC OR SEMI-PUBLIC PLACES UNLESS INSTRUCTED BY YOU TO DO SO."[96] Likewise, Fertility Friend states that the company "does not consider your data for sale or trade in any way. Your data is not a currency at Fertility Friend. . . . Privacy is our focus. We are fully aware of the sensitive nature of your data."[97] The company touts its "privacy-aware procedures" and "clear and ethical business model" because of its awareness that even "anonymized" health information often remains identifiable.[98] Another period tracking website, which also partners with employer-sponsored wellness plans, publicizes that it "does not share personal data that directly identifies you, such as your name or email address, with anyone except people you invite . . . . [W]e do not share your health data with your employer unless you expressly opt-in for a specific purpose . . . ."[99] In addition to promising not to share or sell user data, OvuSense goes as far as selling consumers on the security of its platform, explaining that "data is stored in an encrypted format in the cloud meaning it [sic] secure and cannot be deciphered" and that its "cloud database . . . complies with strict regulatory guidelines which includes [sic] security management to the ISO 27001 standard and personal data protection to the ISO 27018 standard."[100]

Similarly, mental health apps also try to appeal to consumers by using privacy and data security as a selling point. Stress management

---

95 *Glow Privacy Policy*, GLOW, https://glowing.com/privacy-20200331 [https://perma.cc/M5TY-2RN6] (last updated Mar. 31, 2020).

96 *Id.*

97 *Privacy & Clarity*, FERTILITY FRIEND, https://www.fertilityfriend.com/pres/ [https://perma.cc/E7AE-95HU].

98 *Id.*

99 *Ovia Health Apps Privacy Policy*, OVIA HEALTH, https://connect.oviahealth.com/en/privacy-policy.html [https://perma.cc/BQE2-TJX6] (last updated Mar. 23, 2021).

100 *Your OvuSense Questions Answered*, OVUSENSE, https://www.ovusense.com/us/faqs/ [https://perma.cc/KLE4-9V8W] (answering the question, "I'm Worried about my data getting leaked. How is it protected?").

app Moodpath (now MindDoc) tells consumers that "[y]our information will not be passed on to third parties."[101] Daylio, which helps its users track their mood, explains that "[w]e don't send your data to our servers so we don't have the access to your entries" and that "any other third-party app can't read your data."[102] Emotional health assistant Youper makes several promises to consumers, including that "[a]ll [your personal] data are stored in a safe and very restricted cloud infrastructure" that "is not accessible to anyone, for any reason."[103] The company also assures users that it "does not get any personal or monetary gain from your personal information or medical data" and that it definitively does not share your information with others because "[a]ll your information is private."[104] And Peak, a "brain-training" app, tells consumers, "[We] are committed to protecting and respecting your privacy . . . ."[105]

Genetic apps make similar promises to their consumers. For instance, 23andMe tells potential customers, "It's your data, so you call the shots. From the moment you register your kit and set up your private account, you have meaningful choice in everything you do. That means you decide how your information is used and with whom it is shared."[106] AncestryDNA advertises that consumers' privacy "is our highest priority" and that the consumers "own your DNA data . . . [and] can choose to download [raw] DNA Data, have us delete your DNA test results as described in the Ancestry® Privacy Statement, or have us destroy your physical DNA saliva sample."[107] MyHeritage's website states that "your privacy and the security of your data is as important to us as it is to you."[108] It tells users that the company has "made significant investments to ensure that your account and

101 *MindDoc FAQ*, MINDDOC, https://mymoodpath.com/en/frequently-asked-questions/ [https://perma.cc/8JU8-GYAG] (answering the question, "Is my data secure?").

102 *How Secure Is My Data?*, DAYLIO, https://faq.daylio.net/article/48-how-secure-is-my-data [https://perma.cc/Z2MK-BXHF].

103 *How Does Youper Protect My Privacy?*, YOUPER, https://youper.zendesk.com/hc/en-us/articles/360024814031-How-does-Youper-protect-my-privacy- [https://perma.cc/J32R-8JJ9].

104 *Frequently Asked Questions*, YOUPER, https://www.youper.ai/faq [https://perma.cc/P94R-CGU8] (first answering the question, "How does Youper protect my privacy?", then answering, "Is my information shared with others?").

105 *Privacy and Cookie Policy*, PEAK, https://www.peak.net/privacy-policy/ [https://perma.cc/HWQ3-NVU7].

106 *Privacy*, 23ANDME, https://www.23andme.com/privacy/ [https://perma.cc/8H8X-M5L5].

107 *FAQs*, ANCESTRYDNA, https://support.ancestry.com/s/ancestrydna [https://perma.cc/5Q2S-JCU8] (answering "How secure and private is AncestryDNA?").

108 *DNA*, MYHERITAGE, https://www.myheritage.com/dna [https://perma.cc/769D-GR6F].

personal details are secured and protected by multiple layers of encryption."[109]

In sum, health app providers promise their consumers both privacy and data security. The fact that so many digital health tech companies advertise their commitment to privacy illustrates that they believe that their consumers will select products based on these terms.

2. Unilateral Amendment Clauses as Market Failure

While advertisements for digital health tech demonstrate that people may, in fact, shop for privacy when selecting health apps, this market is far from reliable. It fails—in part—because companies often reserve the right to unilaterally amend their ToS and privacy policies, sometimes without even notifying users of the change.

Consider these two examples from the consumer genetics industry. In 2019, FamilyTreeDNA found itself at the heart of a controversy when a news story broke that the allegedly pro-privacy company was allowing law enforcement to search its database for crime-solving purposes.[110] The company informed its customers that it had changed its terms to comply with the European Union's General Data Protection Regulation (GDPR) in May 2018.[111] But sometime in December 2018, FamilyTreeDNA modified its terms of service yet again to allow law enforcement use and failed to notify users. When they found out, FamilyTreeDNA's customers reported feeling betrayed by the company's unannounced change.[112] In the ensuing media frenzy, company president Bennett Greenspan apologized to users and explained that, as of January 2019, it had returned to its earlier policy. His letter promised customers that FamilyTreeDNA "will do a better job communicating with you."[113] The company then changed its terms of service to allow users to opt out of law enforcement matching.[114]

---

109 *Id.*

110 Kristen V. Brown & Bloomberg, *A Major DNA-Testing Company Is Sharing Some of Its Data With the FBI. Here's Where It Draws the Line*, FORTUNE (Feb. 1, 2019), https://fortune.com/2019/02/01/genetic-testing-consumer-dna-familytreedna-fbi/ [https://perma.cc/5UY2-9YE8].

111 Email from Bennett Greenspan, President, FamilyTreeDNA, to Our Customers (2019), https://mailchi.mp/familytreedna/letter-to-customers?e=%20 [https://perma.cc/XN82-CZXF].

112 Matthew Haag, *FamilyTreeDNA Admits to Sharing Genetic Data With F.B.I.*, N.Y. TIMES (Feb. 4, 2019), https://www.nytimes.com/2019/02/04/business/family-tree-dna-fbi.html [https://perma.cc/HD4Y-99NL].

113 Email from Bennett Greenspan to Our Customers, *supra* note 111; *see also* Natalie Ram & Jessica L. Roberts, *Forensic Genealogy and the Power of Defaults*, 37 NATURE BIOTECH. 707, 707–08 (2019).

114 Haag, *supra* note 112. Interestingly, FamilyTreeDNA opted out consumers with EU-based accounts automatically, likely because of the GDPR. Users in the EU must therefore

Around the same time, GEDMatch—the consumer genetic database made famous by the Golden State Killer case—also shared its users' information without their knowledge.[115] As of May 2018, the company's terms explicitly provided for law enforcement matching only for violent crimes, which it defined as sexual assault or homicide.[116] GEDMatch then made an exception and allowed law enforcement to search its database in conjunction with an aggravated assault, only informing users after the fact.[117] Again, public outcry ensued. In May 2019, GEDMatch responded by changing its ToS.[118] Among the updates was an expansion of its definition of violent crime to include aggravated assault and requiring existing users to opt in to law enforcement matching.[119] Even after these changes, GEDMatch opts new users into law enforcement matching by default but allows them to opt out.[120] And even more changes could be on the horizon, as the for-profit forensic genomics company Verogen acquired GEDMatch in December 2019.[121] The company informed its users that if they were uncomfortable with the change, they were free to delete their accounts.

Examples of apps with high risks and numerous users continue to make headlines. These examples demonstrate how even users who completely read and understand a company's ToS and privacy policy may find themselves subject to unwanted uses of their sensitive data.

Consider some of the health app examples above. A user might select OvuSense to track her ovulation over Ava because of OvuSense's stated commitment to data security and adherence to industry standards. But should the company change to a cheaper, less secure data platform, the customer would likely have to choose between diminished data security and abandoning all of her existing information to switch to a new ovulation tracker.[122] Or perhaps

---

opt in to law enforcement matching, unlike their counterparts in the rest of the world. Ram & Roberts, *supra* note 113, at 707.

115 Natalie Ram, *The Genealogy Site That Helped Catch the Golden State Killer Is Grappling With Privacy*, SLATE (May 29, 2019), https://slate.com/technology/2019/05/gedmatch-dna-privacy-update-law-enforcement-genetic-geneology-searches.html [https://perma.cc/3E3S-VRSA]; *see also* Ram & Roberts, *supra* note 113, at 707.

116 *See* Ram, *supra* note 115.

117 *Id.*

118 Ram & Roberts, *supra* note 113, at 707.

119 *See id.*; Ram, *supra* note 115.

120 Ram & Roberts, *supra* note 113, at 707.

121 Nila Bala, *We're Entering a New Phase in Law Enforcement's Use of Consumer Genetic Data*, SLATE (Dec. 19, 2019), https://slate.com/technology/2019/12/gedmatch-verogen-genetic-genealogy-law-enforcement.html [https://perma.cc/EMF6-E5XF].

122 Of course, if people had ownership rights in their data, they could take it with them from platform to platform. For arguments in favor of genetic ownership rights, see generally Jessica L. Roberts, *Progressive Genetic Ownership*, 93 NOTRE DAME L. REV. 1105

another consumer selects Daylio instead of Vent to log her moods because of the assurance that no third parties will have access to her entries. If a company that wishes to monetize user data acquires Daylio, the user will again probably have to decide whether to stop using the service—and lose access to her data in the process—or agree to the new, less desirable ToS or privacy policy.

Sadly, we cannot depend on public outcry like what occurred in the consumer genetics controversies to police harmful one-sided changes. Many of these changes could occur without consumers' knowledge. As described below, when companies reserve the right to make unilateral amendments, they often do so with no obligation to actually inform their users.[123]

One might think that the market for privacy itself could be a check on unfavorable unilateral amendments. However, that might not be the case. Companies could use desirable privacy terms to lure consumers in and then, when they have a critical mass of users, change those terms to profit from the data. Because of the status quo bias and high switching costs described in Part II,[124] even current users who dislike the new terms will be inclined to keep using the app. Consider this example. In 2015, 23andMe shocked consumers by signing the first of many lucrative agreements to give pharmaceutical and biotech companies access to its customer database.[125] The users whose data it sold had agreed to donate their genetic information for research purposes.[126] Nonetheless, they felt deceived that the company profited from something that they gave away for free.[127] While customers felt surprised, commentators were not. Many had long suspected that 23andMe's true business model was not selling genetic tests but

(2018), and Jessica L. Roberts, *In Favor of an Action for Genetic Conversion*, *in* CONSUMER GENETIC TECHNOLOGIES: ETHICAL AND LEGAL CONSIDERATIONS 39 (I. Glenn Cohen, Nita A. Farahany, Henry T. Greely & Carmel Shachar eds., 2021).

123 *See infra* Section II.A.

124 *See infra* Section II.B.

125 Matthew Herper, *Surprise! With $60 Million Dollar Genentech Deal, 23andMe Has a Business Plan*, FORBES (Jan. 6, 2015), http://www.forbes.com/sites/matthewherper/2015/01/06/surprise-with-60-million-genentech-deal-23andme-has-a-business-plan/ [https://perma.cc/63GD-DYSX].

126 *Id.* According to the company, eighty percent of its customers consent to sharing their genetic data. Lydia Ramsey, *23andMe CEO Defends Practice of Sharing Genetic Info with Pharma Companies*, YAHOO! FIN. (July 7, 2015), http://finance.yahoo.com/news/23andme-ceo-defends-practice-sharing-164857907.html [https://perma.cc/EA7K-TGG3].

127 *See, e.g.*, Jessica L. Roberts, Theories of Genetic Ownership 2 (Sept. 9, 2015) (unpublished manuscript), https://petrieflom.law.harvard.edu/events/details/health-law-workshop-jessica-l-roberts [https://perma.cc/5T5Z-3EPF] (discussing January 8, 2015, response of one commenter, William Chang, who stated: "I would have thought that donating my genome meant that it would be donated, not sold, for research.").

brokering genetic data.[128] It is probably no coincidence that the company waited until it had hundreds of thousands of users *before* announcing its intention to sell their data. Instead of relying on a research consent provision, a health app could similarly amass large amounts of consumer information using favorable privacy terms, then unilaterally amend its ToS and privacy policies to allow it to sell that data to third parties. And, depending on the users' abilities to delete their profiles, even consumers who stopped using the health app after the change might be powerless to stop the company from selling the data that it had already collected from them.

C. Ubiquity of Unilateral Amendment Clauses

Unilateral amendment clauses are ubiquitous. To assess the frequency of these provisions, we conducted a survey of the terms of service and privacy policies for thirty different health apps, ten from each of our three categories.[129] For every app, we downloaded and analyzed the content of both the ToS and the privacy policy. When possible, we analyzed the unilateral amendment clauses in ToS and privacy policies separately.

All of the health apps that we surveyed reserve the right to make one-sided changes to their ToS, to their privacy policies, or both, sometimes without notifying users. Regarding ToS, 100% (10/10) of genetics apps, 80% (8/10) of femtech apps, and 70% (7/10) of mental health apps contained unilateral amendment clauses. The privacy policies for all thirty health apps included in this study contained unilateral amendment language.

---

128 *See* Charles Seife, *23andMe Is Terrifying, But Not for the Reasons the FDA Thinks*, SCI. AM. (Nov. 27, 2013), http://www.scientificamerican.com/article/23andme-is-terrifying-but-not-for-reasons-fda/ [https://perma.cc/G2AN-FP8W]; *see also* David P. Hamilton, *23andMe: Will the Personal-Genomics Company Need Big Pharma to Make Money?*, VENTUREBEAT (Nov. 19, 2007), http://venturebeat.com/2007/11/19/23andme-will-the-personal-genomics-company-need-big-pharma-to-make-money/ [https://perma.cc/9E3Z-3NFF]. One article warned consumers, "If you're paying a cut rate to have 23andMe sequence your DNA, you are 23andMe's product." Sarah Zhang, *Of Course 23andMe's Plan Has Been to Sell Your Genetic Data All Along*, GIZMODO (Jan. 6, 2015), http://gizmodo.com/of-course-23andmes-business-plan-has-been-to-sell-your-1677810999 [https://perma.cc/VAE4-SJLH].

129 For details on our methodology, including how we selected the thirty apps in our study, please see *infra*, Appendix.

TABLE 1: UNILATERAL AMENDMENT PROVISIONS

App Type	UA in ToS	UA in PP
Genetic	10/10 (100%)	10/10 (100%)
Femtech	8/10 (80%)	10/10 (100%)
Mental Health	7/10 (70%)	10/10 (100%)
Totals	25/30 (~83%)	30/30 (100%)

Apps vary with respect to informing users of one-sided changes. Some apps may put an "updated" label next to the relevant link on their website or change the "last updated" text at the top or bottom of the document. Other apps take a more proactive approach, either through in-app pop-ups or by emailing users.[130] For ToS, 60% (6/10) of genetics apps, approximately 63% (5/8) of femtech apps, and approximately 71% (5/7) of mental health apps promised to notify users in some way. For privacy policies, 100% (10/10) of genetics apps, 70% (7/10) of femtech apps, and 70% (7/10) of mental health apps indicated that they would notify users of modifications. Interestingly, some apps, like DNA2Tree, specifically tell users that they "waive any right to receive specific notice of each such change."[131]

TABLE 2: ALL APPS

App Type	Will Notify ToS	Will Notify PP
Genetic	6/10 (60%)	10/10 (100%)
Femtech	5/8 (~63%)	7/10 (70%)
Mental Health	5/7 (~71%)	7/10 (70%)
Totals	16/25 (64%)	24/30 (80%)

Of the apps that promised to inform users of updates, some only agreed to notify if the change was "material."[132] Apps—not their users—determine whether a change is material, yet no apps defined that term. All of Us opted for less-legal language, noting that "[i]f we make big changes, we will try to tell you directly."[133] For ToS, 20%

130 If an app indicated that it would attempt to draw attention to changes in any way, regardless of how minimal, we coded it as intending to notify users. If an app characterized merely posting new ToS or privacy policies as notification without a "last modified" date, we did not code it as notifying users.

131 *Terms of Use*, DNA2TREE, https://web.archive.org/web/20200220223434/http://dnadreamers.com/terms/ (last visited Sept. 24, 2021).

132 *See, e.g.*, *Terms of Service*, 23ANDME (Sept. 30, 2019), https://www.23andme.com/about/tos/ [https://perma.cc/UM5L-TQ8L]. We coded these apps as "discretionary."

133 All of Us *Research Program Website and App Privacy Policy*, ALL OF US, https://www.joinallofus.org/privacy-policy# [https://perma.cc/VZS7-ZL7N].

(2/10) of genetics apps, approximately 63% (5/8) of femtech apps, and approximately 43% (3/7) of mental health apps indicated that they would notify users of material changes over email. For privacy policies, 70% (7/10) of genetics apps, 30% (3/10) of femtech apps, and 20% (2/10) of mental health apps indicated that they would notify users via email in the event of a material change.

TABLE 3: DISCRETIONARY NOTIFICATION[134]

App Type	Will Email ToS	Will Email PP
Genetic	2/10 (20%)	7/10 (70%)
Femtech	5/8 (~63%)	3/10 (30%)
Mental Health	3/7 (~43%)	2/10 (20%)
Totals	10/25 (40%)	12/30 (40%)

While some agree to notify consumers, many apps charge users themselves with reviewing the ToS and privacy policies for possible updates.[135] In ToS containing unilateral amendments, 60% (6/10) of genetics apps, approximately 63% (5/8) of femtech apps, and about 14% (1/7) of mental health apps instruct users to check back for the most current language. In privacy policies, 40% (4/10) of genetics apps, 70% (7/10) of femtech apps, and 70% (7/10) of mental health apps include language telling users to review those policies regularly.

TABLE 4: USER RESPONSIBILITY

App Type	Check Back ToS	Check Back PP
Genetic	6/10 (60%)	4/10 (40%)
Femtech	5/8 (~63%)	7/10 (70%)
Mental Health	1/7 (~14%)	7/10 (70%)
Totals	12/25 (48%)	18/30 (60%)

Finally, we provide a note on users' abilities to accept or reject new terms. The majority of apps consider continued use acceptance. In ToS, 90% (9/10) of genetics apps, approximately 63% (5/8) of femtech apps, and approximately 71% (5/7) of mental health apps explicitly state that using the app after the modification demonstrates acceptance of the new terms. One mental health app included in this statistic, Vent, notes that a user "will be given the opportunity to accept such varied Terms on [his or her] first visit to the Site after such

134 Tables only include apps promising to notify consumers of material changes.

135 We coded unilateral amendment provisions to see which apps explicitly stated this expectation.

variation occurs."[136] In privacy policies, 70% (7/10) of genetics apps, 40% (4/10) of femtech apps, and 10% (1/10) of mental health apps indicate that the apps would construe continued use as acceptance of the modification. The remaining apps were silent on how users indicate acceptance.

TABLE 5: ACCEPTANCE OF MODIFIED TERMS

App Type	Continued Use ToS	Continued Use PP
Genetic	9/10 (90%)	7/10 (70%)
Femtech	5/8 (~63%)	4/10 (40%)
Mental Health	5/7 (~71%)	1/10 (10%)
Totals	19/25 (76%)	12/30 (40%)

Perhaps troublingly, the vast majority of apps do not allow a consumer to reject one-sided changes. None of the apps in this study allow users to object to changes to privacy policies. Perhaps surprisingly, three apps do allow users—at least theoretically—to contest a change to the ToS. Clue gives users of its subscription service a "right to object to the amendment of the Agreement within an adequate amount of time" when they receive notice of the amendment.[137] Moodpath (now MindDoc) reserves the right to make changes to terms and conditions "unless [it] is unreasonable for the user" and notes that a user can "object within [a] 6-week period."[138] 23andMe states that "[u]nless you notify us within thirty (30) days from the time you receive notice of the new terms that you do not agree to the terms, you will be deemed to have agreed to the new TOS."[139]

Although none of the ToS explained what would happen should a user object to a modification, a consumer might reasonably expect that these provisions hold special meaning. To clarify, we emailed customer service for the three apps that allow consumers to reject new terms. 23andMe stated that if a user does not want to accept the updated terms, she may, like all users, delete her account and personal data.[140] Moodpath responded that "It is indeed true that if you object to the changes, the only option would be to cease using the service."[141] These results suggest that "objection" language does not confer actual

136 *Terms of Service*, VENT, https://www.vent.co/tos/ [https://perma.cc/HRV6-KKZT].

137 *Terms of Service*, CLUE (Aug. 2, 2017), https://web.archive.org/web/20191202231944/https://helloclue.com/terms (also on file with authors).

138 *General Terms and Conditions*, MINDDOC, https://mymoodpath.com/en/terms-services/ [https://perma.cc/X7K7-SKR6].

139 *Terms of Service*, *supra* note 132.

140 Correspondence on file with authors.

141 Correspondence on file with authors.

legal rights to the user. Instead, it may deceive her into choosing an app based on the incorrect assumption that she can opt out of unfavorable changes without having to stop using the app when she, in fact, cannot. Clue, however, is a notable outlier. They responded that paid subscribers—although not users who use the app for free—*can* opt out of changes that they deem objectionable and that those changes will not apply to them.[142] Effectively, those users pay a premium to reject one-sided changes as part of their subscription fee.

To sum up, the results of our study of unilateral amendments indicate that these provisions are near-universal in the ToS and privacy policies of digital health tech companies. While most health apps promise to notify users of at least some updates, many companies place the responsibility of staying informed with the individual user. Complicating the situation further, continuing to use the service may constitute legal acceptance of new terms. Only one company appears to allow consumers to opt out of new terms while continuing to use the app, and that option is only available to paying users.

* * *

Although consumers may not shop for terms, health apps attract users by advertising their commitment to privacy and data security. Digital health tech consumers might then select one service over another based on the company's vow to safeguard its users' data. Yet this market for privacy is unstable due, in part, to the ability of companies to make one-sided changes, sometimes without even notifying users. Our research finds that unilateral amendment clauses are ubiquitous in the digital health tech industry. If a company changes its ToS or privacy policy in a way that compromises users, consumers must decide between using potentially beneficial health apps and accepting unfavorable new terms. Unilateral amendment clauses, therefore, distort the market for privacy. In the following Part, we turn to the law governing unilateral amendments by health apps and consider why one-sided changes could raise particularly problematic concerns in the context of digital health tech.

II. REGULATING DIGITAL HEALTH TECH

Health app users may value privacy more than the average consumer. But the near-universal prevalence of unilateral amendment clauses undermines their ability to reliably shop for privacy terms. This Part examines the legal mechanisms for protecting users of digital health tech against unfavorable one-sided changes that could

142 Correspondence on file with authors.

compromise their privacy. Perhaps surprisingly, the major federal laws and regulations designed to safeguard health-related data simply do not apply to many direct-to-consumer health apps. This regulatory gap means that courts will likely turn to run-of-the-mill contract law and consumer law to resolve legal disputes.[143] Sadly, these bodies of law currently offer health app consumers little meaningful protection. Building on the scholarship that has criticized unilateral amendments as a general matter, we argue that allowing one-sided changes to the ToS and privacy policies is particularly dangerous in the context of digital health tech. We therefore conclude that the current state of the law leaves health app users highly vulnerable.

A. Current Law

Here we outline the existing law that would apply if health app users legally challenged a one-sided change that violated their privacy. While one might reasonably assume that medical privacy laws and regulations could offer some protection, these safeguards often do not apply outside the traditional health care context. Because many digital health tech companies are not providing health care per se, they escape regulation. Instead, health app users must rely on contract and consumer law doctrines to challenge one-sided changes. However, as we discuss below, the very same kinds of unilateral amendments clauses that we deemed problematic in the preceding Part are hard to challenge under those bodies of law.

1. Health Law and Regulation

In the absence of a comprehensive data protection statute, American consumers must rely on fragmented, industry-specific laws and regulations.[144] The financial sector has one set of consumer privacy protections, and health care—at least in certain contexts—has another.[145] Many of the health apps described in Part I unequivocally collect health-related data. Consumers might then expect the traditional safeguards present in health care likewise to apply here. This assumption, unfortunately, is incorrect.[146]

143 *See* Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 N.Y.U. L. REV. 662, 663 (2019).

144 Nicolas P. Terry, *Assessing the Thin Regulation of Consumer-Facing Health Technologies*, 48 J.L. MED. & ETHICS (SPECIAL SUPP. 48:1) 94, 95 (2020).

145 *Id.*

146 We confine our analysis here to federal health laws and regulations. However, some state laws may apply. *See* Stacey A. Tovino, *Going Rogue: Mobile Research Applications and the Right to Privacy*, 95 NOTRE DAME L. REV. 155, 190–206 (2019); *see also* Mark A. Rothstein et

The major federal laws and regulations that protect medical data in the United States apply specifically to "health care." Despite offering health-related services and collecting health-related information, many health apps do not actually provide health care in the legal sense, and digital health tech companies are explicit about that fact. Direct-to-consumer health apps frequently include medical disclaimers in their ToS. This language might read as "this [s]oftware is not intended to be a substitute for professional medical advice, diagnosis, or treatment," and "[r]eliance on any information provided by [the app] . . . is solely at your own risk."[147] In other words, most users of health apps are not "patients" but merely "consumers." As a result, many of those technologies do not have to comply with the Health Insurance Portability and Accountability Act (HIPAA) or face Food and Drug Administration (FDA) regulation.[148]

a. HIPAA Privacy Rule

The HIPAA Privacy Rule lays out standards for using and disclosing a person's individually identifiable health information.[149] The statute only covers health care providers, health plans, health care clearinghouses, and their business associates.[150] HIPAA will then apply to data stored in health apps offered by those entities[151] but not to similar technologies made by private companies to sell directly to consumers.[152] Because data are nonrivalrous—the same information can exist simultaneously in two places at once—the exact same data point, say the date of a person's last menstrual period, can simultaneously have HIPAA protection (stored in an electronic medical record at her obstetrician's office) and not have HIPAA protection (entered into a direct-to-consumer femtech app).[153]

Complicating matters even more, regardless of whether a health care provider initially collected the data, once the consumer downloads the information to a third-party platform, HIPAA may no

al., *Unregulated Health Research Using Mobile Devices: Ethical Considerations and Policy Recommendations*, 48 J.L. MED. & ETHICS (SPECIAL SUPP. 48:1) 196, 209–10 (2020).

147 *Terms of Use*, DAYLIO, https://faq.daylio.net/article/32-terms-of-use [https://perma.cc/NEX3-93WR].

148 The Federal Trade Commission maintains an online tool to help determine if an app is subject to HIPAA; the Federal Food, Drug, and Cosmetic Act (FD&C Act); the FTC Act; or other laws. *Mobile Health Apps Interactive Tool*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool [https://perma.cc/XE7W-NF4G] (last updated Apr. 2016).

149 45 C.F.R. § 164.502 (2020).

150 *Id.* § 164.104.

151 *Id.* § 160.103.

152 Terry, *supra* note 144, at 95.

153 *See id.* at 94.

longer apply. Perhaps troublingly, these kinds of consumer products already exist, and recent regulatory changes are making it easier for private companies to gain access to people's medical records. Industry giants Google and Apple have both developed products for consumers to store their medical records and other health data in a single place.[154] Furthermore, recently implemented regulations allow app developers to receive patient information directly from health care providers.[155] Supporters applaud these developments as empowering consumers to store and share their health data without physician involvement, giving individuals better control over their medical information.[156] One potentially underappreciated consequence is that otherwise protected health data will fall outside the scope of medical privacy law. In other words, HIPAA's Privacy Rule will cover your medical records stored in MyChart[157] but not on Apple Healthcare or Google Health.[158]

Regardless of whether a health app user uploads her data from her health care provider or inputs it herself, HIPAA will not protect that information in most direct-to-consumer health apps.

b. FDA Oversight

Additionally, many health apps also fall outside the scope of the FDA's authority. The FDA protects public health by regulating the safety, quality, and effectiveness of a variety of products, including food, drugs, biologics, and medical devices. The agency regulates certain kinds of health-related software as medical devices, which could include some consumer health apps.[159]

To be sure, a few health apps have actually sought FDA approval. For example, Natural Cycles is a fertility tracking app that has been

154 *Apple Healthcare*, APPLE, https://www.apple.com/healthcare/health-records/ [https://perma.cc/F4VT-SRL8]; *Google Health*, GOOGLE, https://health.google/ [https://perma.cc/JGN9-Y4LG].

155 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25642, 25647 (May 1, 2020) (to be codified at 45 C.F.R. pts. 170, 171); Interoperability and Patient Access, 85 Fed. Reg. 25510, 25511 (May 1, 2020) (to be codified at 42 C.F.R. pts. 406, 407, 422, 423, 431, 438, 457, 482, 485 and 45 C.F.R. pt.156).

156 Anna Wilde Mathews & Melanie Evans, *Sharing Your Digital Health Data: New Rules Ease Access*, WALL ST. J. (Mar. 9, 2020), https://www.wsj.com/articles/sharingyourhealthdatanewdigitalrules-11583702453 [https://perma.cc/25JB-27DJ].

157 *See Connect to Your Provider*, MYCHART, https://www.mychart.com/LoginSignup [https://perma.cc/4DR8-A3J4]; *see also MyChart*, APPLE, https://apps.apple.com/us/app/mychart/id382952264 [https://perma.cc/27RY-CXVA].

158 *See Apple Healthcare*, *supra* note 154; *Google Health*, *supra* note 154.

159 U.S. FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4–5 (2019).

cleared by the FDA for marketing as contraception.[160] 23andMe—after the FDA shut down the company's early efforts to provide health-related information to its customers in 2013[161]—has since obtained FDA approval for some of its tests for measuring health risk[162] and assessing how users metabolize certain drugs.[163] Likewise, some mental health apps may qualify as "[s]oftware functions that help patients with diagnosed psychiatric conditions," which the FDA can regulate at its discretion.[164]

Nonetheless, much of digital health tech eludes FDA regulation. The definition of medical "device" in the 21st Century Cures Act, federal legislation designed to fund precision medicine efforts and to improve healthcare technology, excludes software intended "for maintaining or encouraging a healthy lifestyle and is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition" from regulation.[165] The FDA has further clarified that this carve-out includes "low risk" wellness apps intended to promote, track, or encourage a healthy lifestyle.[166] The result is that only a minority of health apps are subject to FDA oversight.

Of course, the FDA concerns itself primarily with safety, not privacy. While the agency does not directly assess the data risks of the devices it regulates, the FDA has taken some nonbinding measures to demonstrate its commitment to improving data security.[167] Should the agency decide to do more in this area, it will only have limited authority over most direct-to-consumer health apps.

---

160 *FDA Allows Marketing of First Direct-to-Consumer App for Contraceptive Use to Prevent Pregnancy*, U.S. FOOD & DRUG ADMIN. (Aug. 10, 2018), https://www.fda.gov/news-events/press-announcements/fda-allows-marketing-first-direct-consumer-app-contraceptive-use-prevent-pregnancy [https://perma.cc/Z66V-3Y9G].

161 GlobalData Thematic Research, *Timeline: The Development of Genomic Sequencing Technology*, PHARM. TECH. (Jan. 27, 2021), https://www.pharmaceutical-technology.com/comment/genomics-timeline/ [https://perma.cc/K34P-JU53].

162 *23andMe and the FDA*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/211831908-23andMe-and-the-FDA [https://perma.cc/M2PR-CKNF].

163 *23andMe Granted the First and Only FDA Authorization for Direct-to-Consumer Pharmacogenetic Reports*, 23ANDME (Nov. 1, 2018), https://mediacenter.23andme.com/press-releases/23andme-granted-the-first-and-only-fda-authorization-for-direct-to-consumer-pharmacogenetic-reports/ [https://perma.cc/JW5V-NBBU].

164 *Examples of Software Functions for Which the FDA Will Exercise Enforcement Discretion*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/device-software-functions-including-mobile-medical-applications/examples-software-functions-which-fda-will-exercise-enforcement-discretion [https://perma.cc/QS8Q-HE2Z] (last updated Sept. 26, 2019).

165 21st Century Cures Act, Pub. L. No. 114–255, § 3060, 130 Stat. 1130, 1130 (2016).

166 U.S. FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES 4 (2019); *see also* 21st Century Cures Act § 3060; Jeffrey Shuren, Bakul Patel & Scott Gottlieb, *FDA Regulation of Mobile Medical Apps*, 320 JAMA 337, 337 (2018).

167 Terry, *supra* note 144, at 97.

2. Contract Law

Health app users that want to challenge unilateral amendments will likely have to turn to ordinary contract law and its application to ToS and privacy policies. Those documents outline a company's promises to customers. ToS are generally enforceable as contracts. Despite "bear[ing] all of the earmarks of a contract,"[168] whether privacy policies are contracts is debatable.[169] At the very least, they are "quasi-contractual statements."[170] Absent other intervening laws and regulations, ToS and privacy policies likely govern any disputes between digital health tech companies and their users.

Unfortunately for consumers, courts may not be willing to police unilateral amendments using contract law. In *Tompkins v. 23andMe, Inc.*, a class of plaintiffs brought claims against 23andMe for "unfair business practices, breach of warranty, and misrepresentations about the health benefits of 23AndMe's services."[171] The court held that plaintiffs failed to demonstrate that the ability to make one-sided changes rendered the arbitration clause, which appeared in a separate provision, unconscionable.[172] Thus, courts may be willing to enforce the unilateral amendment provisions in the ToS of health apps.

We explain below how a variety of contract law doctrines could theoretically protect health app users from unfavorable one-sided changes. Nevertheless, courts have been inconsistent when applying these doctrinal tools, each of which suffers from serious limitations.

a. Illusory Promises

First, courts might deem ToS containing unilateral amendment provisions illusory. According to this reasoning, if the party seeking to enforce the contract can modify the agreement as it pleases, it has effectively made no legally enforceable promise.[173] For instance, in *Dumais v. American Golf Corp.*, the court held that an employment contract's arbitration agreement, which allowed the employer to "at any time change, delete, modify, or add to any of the provisions

168 Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 91 (1999).

169 For an excellent discussion, see Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 595–97 (2014).

170 James Fallows Tierney, *Contract Design in the Shadow of Regulation*, 98 NEB. L. REV. 874, 889 (2020).

171 Tompkins v. 23andMe, Inc., 840 F.3d 1016, 1021 (9th Cir. 2016).

172 *Id.* at 1033. The court also found that the plaintiffs failed to establish the unconscionability of the bilateral prevailing party clause, the forum selection clause, and the clause excluding intellectual property claims from arbitration unconscionable. *Id.* at 1025, 1029, 1031.

173 Nat'l Fed'n of the Blind v. The Container Store, Inc., 904 F.3d 70, 87 (1st Cir. 2018).

contained in this handbook at its sole discretion," was illusory because it allowed "one party the unfettered right to alter the arbitration agreement's existence or its scope."[174]

Unfortunately, declaring a contract is illusory and unenforceable is faint protection for health tech consumers *who want to enforce* companies' initial promises for privacy protections. If a court throws out the contract, it throws out the baby of privacy protections with the bathwater of unilateral amendment clauses. Another problem with relying on illusory promises is that some courts have held that unilateral amendment provisions are enforceable and are not illusory, so courts are not consistent even in applying this doctrine.[175] Moreover, other courts hold that because the parties make other promises in a contract that are unrelated to the unilateral amendment provision, contracts with these types of provisions are still supported by consideration.[176] So, the reach of cases like *Dumais* is limited in addition to being unhelpful in protecting consumers.

b. Unconscionability

Second, unconscionability could prevent companies from changing ToS.[177] Unconscionability exists in two forms: (1) procedural and (2) substantive. Procedural unconscionability stems from the unfairness of the bargaining process. Substantive unconscionability speaks to the terms themselves. Several courts have held that clauses reserving the right to unilaterally amend a contract make contracts procedurally unconscionable. For instance, in *Merkin v. Vonage American Inc.*, the court found that the company's ability to make one-sided changes, which it regularly exercised, "transformed an ordinary contract of adhesion into a contract that gave Vonage the largely unfettered power to control the terms of its relationship with its subscribers."[178] The unilateral amendment clause was, according to the court, one "indici[um] of oppression."[179] Thus, cases like *Merkin*

174 Dumais v. Am. Golf Corp., 299 F.3d 1216, 1217, 1219 (10th Cir. 2002) ("[An] ability to modify rules 'in whole or in part' without notice to employee renders arbitration agreement illusory." (quoting Hooters of Am., Inc. v. Phillips, 173 F.3d 933, 939 (4th Cir. 1999))).

175 *See, e.g.*, Blair v. Scott Specialty Gases, 283 F.3d 595, 604 (3d Cir. 2002); Yufan Zhang v. UnitedHealth Grp., 367 F. Supp. 3d 910, 916 (D. Minn. 2019); Taylor v. First N. Am. Nat'l Bank, 325 F. Supp. 2d 1304, 1314–15, 1315 n.18 (M.D. Ala. 2004).

176 Carroll v. Stryker Corp., 658 F.3d 675, 683 (7th Cir. 2011).

177 Oren Bar-Gill & Kevin Davis, *Empty Promises*, 84 S. CAL. L. REV. 1, 31 (2010).

178 Merkin v. Vonage Am. Inc., No. 13-CV-08026, 2014 WL 457942, at *7 (C.D. Cal. Feb. 3, 2014), *rev'd*, No. 14-55397, 2016 WL 775620 (9th Cir. Feb. 29, 2016), *opinion withdrawn and rev'g trial court* 639 F. App'x 481 (9th Cir. 2016).

179 *Id.*

might appear to offer some hope for health tech consumers challenging one-sided changes.

Procedural unconscionability is not, however, a sure thing. Courts may allow minimal amount of notice to prevent a unilateral modification provision from being procedurally unconscionable. For example, in *Klein v. Verizon Communications, Inc.*, the court found that an email notice of changes and the right to cancel the service were sufficient to overcome procedural unconscionability.[180] Thus, health apps could simply send a mass email when they make one-sided changes, which many already promise to do. By contrast, apps that require users themselves to monitor the ToS and privacy policies for changes may face procedural unconscionability.

And even favorable precedents for procedural unconscionability may only go so far. Some jurisdictions require both procedural *and* substantive unconscionability to invalidate a contract term. Thus, courts may find that, while a provision may be *procedurally* unconscionable, it is not *substantively* unconscionable and is therefore enforceable, like in *Tompkins v. 23andMe, Inc.*.[181] Another court dismissed the application of substantive unconscionability to a unilateral amendment provision outright, saying "courts routinely enforce such terms in form contracts."[182] This finding is not terribly surprising, given that the doctrine of substantive unconscionability tends to rely heavily on plaintiff-unfriendly industry norms.[183]

Furthermore, unconscionability doctrine over the past few decades has focused on arbitration agreements.[184] The mere fact that courts might prevent unilateral amendments to arbitration clauses should not comfort consumers who face companies changing terms unrelated to arbitration. Moreover, the extent to which these decisions apply to privacy policies versus ToS remains unclear. In fact, we could not locate a single case where a court invalidated a unilateral amendment to a privacy policy.[185]

---

180 Klein v. Verizon Commc'ns, Inc., 920 F. Supp. 2d 670, 673 (E.D. Va. 2013), *rev'd and remanded*, 674 Fed. App'x 304 (2017).

181 Tompkins v. 23andMe, Inc., No. 13-CV-05682, 2014 WL 2903752, at *15 (N.D. Cal. June 25, 2014), *aff'd*, 840 F.3d 1016 (9th Cir. 2016).

182 Song Fi, Inc. v. Google Inc., 72 F. Supp. 3d 53, 63 (D.D.C. 2014).

183 Dov Waisman, *Preserving Substantive Unconscionability*, 44 SW. L. REV. 297, 298–299 (2014).

184 *See* Charles L. Knapp, *Blowing the Whistle on Mandatory Arbitration: Unconscionability as a Signaling Device*, 46 SAN DIEGO L. REV. 609, 622 (2009). *But see* Jacob Hale Russell, *Unconscionability's Greatly Exaggerated Death*, 53 U.C. DAVIS L. REV. 965, 965 (2019) (arguing that unconscionability "is quietly flourishing, and courts regularly use it to strike down substantive terms").

185 For instance, one Westlaw search ("unilateral" AND "amend!" /s "privacy policy") on March 29, 2020 yielded four results, none of which are relevant.

Finally, even in its most robust forms, unconscionability will not give health app users the protection that they need. Unconscionability is usually only a defense to a breach of contract claim.[186] Health app users who wish to challenge a harmful one-sided change are not defending a breach but rather seeking to *enforce* the prior, more favorable terms. In this context, the company compromising data—not the consumer—is likely to be the only party breaching the contract. Health app users do not need a shield to breach of contract. They need a sword to enforce the previous terms.[187] Thus, unconscionability, even at its apex, may be of little use to consumers of digital health tech.

c. The Preexisting Duty Rule

Third, a consumer might appeal to the common law's preexisting duty rule in hopes of defeating a unilateral amendment. Section 73 of the *Restatement (Second) of Contracts* summarizes the rule: "Performance of a legal duty owed to a promisor which is neither doubtful nor the subject of honest dispute is not consideration; but a similar performance is consideration if it differs from what was required by the duty in a way which reflects more than a pretense of bargain."[188] On its face, this appears to make health apps' unilateral amendments unenforceable because the health apps give no consideration for the change (and continue to perform as required by the agreement) but obtain new rights or advantages through amendments.

In reality, however, the preexisting duty rule probably offers little hope to consumers. While formally a rule relating to the doctrine of consideration, the preexisting duty rule is actually a mechanism courts use to police agreements obtained through duress. The comments to Section 89 explain, "The rule of § 73 finds its modern justification in cases of promises made by mistake or induced by unfair pressure. Its application to cases where those elements are absent has been much criticized . . . ."[189] Because of the importance of duress and mistake in preexisting duty rule cases, consumers will likely have to show misconduct on the part of the health app to benefit from the preexisting duty rule, and in many cases, evidence of misconduct will be difficult to produce.

186 Curtis Bridgeman & Karen Sandrik, *Bullshit Promises*, 76 TENN. L. REV. 379, 397 (2009).

187 NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS 65–67, 71–76 (2013).

188 RESTATEMENT (SECOND) OF CONTRACTS § 73 (AM. L. INST. 1981).

189 *Id.* § 89 cmt. b.

d. Promissory Fraud

A final potential doctrine for protecting health tech consumers from undesirable one-sided changes is promissory fraud. This doctrine holds parties liable if they make promises without the intent to keep them. Establishing promissory fraud currently requires that consumers prove that the companies actually intended to deceive them, which can be a challenging burden to carry.

Some legal scholars have suggested modifying promissory fraud by dropping that requirement and replacing it with the lesser showing that the defendant lacked "the intention to perform that its promise implied."[190] Unilateral amendment clauses would be "strong[] prima facie evidence" of the absence of that intent under this proposal.[191] Unlike the existing doctrine of promissory fraud and laws prohibiting bait-and-switch tactics, this change would hold parties liable for merely keeping the option of not performing open.[192] While potentially promising as a means for combatting unfavorable one-sided changes, this approach still has its problems. First, it deviates significantly from well-established legal precedent.[193] And second, consumers will still have the burden of establishing the lack of an intent to perform, which could prove difficult.[194] Thus, like illusory promises and unconscionability, promissory fraud—in both its current and its hypothetical forms—does not do reliable work protecting health tech consumers from undesirable one-sided changes.

3. Consumer Law

Beyond traditional contract law, certain consumer protections may also apply to the agreements between health apps and their users. As with contract law, we conclude that the current legal safeguards fail to adequately protect the users of digital health tech against unfavorable one-sided changes.

a. FTC Oversight

While largely outside the scope of the FDA, as providers of commercial services, digital health tech companies are subject to the

190 Bridgeman & Sandrik, *supra* note 186, at 399.

191 *Id.*

192 *Id.* at 398–400.

193 RESTATEMENT (SECOND) OF TORTS § 526 (AM. L. INST. 1977).

194 Bridgeman & Sandrik, *supra* note 186, at 399 (noting that even under their modified approach, "[o]f course, proving the lack of intention to perform could be difficult . . . .").

oversight of another federal agency: the Federal Trade Commission.[195] As noted in the Introduction, the FTC protects consumers against "anticompetitive, deceptive, and unfair business practices."[196] Specifically, it can intervene on behalf of consumers to stop predatory and misleading conduct in the marketplace. The agency has already intervened in other contexts to secure customers' data as part of its regulation of unfair business practices.[197]

Importantly, the FTC has shown a commitment to consumer privacy, including in digital health tech. Take, for example, the recent complaint against Flo described in the Introduction.[198] Flo's settlement with the FTC required that, among other things, the app "obtain an independent review of its privacy practices and get app users' consent before sharing their health information."[199] As the Director of the FTC's Bureau of Consumer Protection noted in the press release, "[a]pps that collect, use, and share sensitive health information can provide valuable services, but consumers need to be able to trust these apps," so the FTC is "looking closely at whether developers of health apps are keeping their promises and handling sensitive health information responsibly."[200] Likewise, should health apps continue to advertise privacy after changing their terms, the FTC could go after them for misleading consumers. Decades' worth of efforts like the Flo settlement—which go beyond simply enforcing a company's privacy policy—have generated what Professors Daniel Solove and Woody Hartzog call a "common law of privacy" through both judicial decisions and settlement agreements.[201] Recall, however, that the FTC took action against Flo based on its deceptive practices, not harmful one-sided changes.

---

195 Jennifer K. Wagner has persuasively argued that "the FTC is the agency uniquely situated, capable, and qualified to address the challenges raised by technological innovations." Wagner, *supra* note 25, at 105; *see also* Sarah Duranske, *This Article Makes You Smarter! (or, Regulating Health and Wellness Claims)*, 43 AM. J.L. & MED. 7 (2017).

196 *About the FTC*, *supra* note 11.

197 *FTC v. Wyndham*, EPIC, https://epic.org/amicus/ftc/wyndham/ [https://perma.cc/5NJ7-CRM3]; Rafael Reyneri, *Eleventh Circuit LabMD Decision Potentially Limits FTC's Remedial Powers*, COVINGTON: INSIDE PRIVACY (June 11, 2018), https://www.insideprivacy.com/united-states/federal-trade-commission/eleventh-circuit-labmd-decision-potentially-limits-ftcs-remedial-powers/ [https://perma.cc/5U75-ZM7E].

198 Flo Consent Order, *supra* note 1.

199 *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations That It Misled Consumers About the Disclosure of Their Health Data*, FED. TRADE COMM'N (Jan. 13, 2021), https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc [https://perma.cc/M66N-TETR].

200 *Id.*

201 Solove & Hartzog, *supra* note 169, at 583, 585 (noting that "companies look to [FTC settlement] agreements to guide their decisions regarding privacy practices," just as one might look to judicial decisions).

Promisingly, the FTC has shown a willingness to challenge the fairness of one-sided changes in the past. The agency filed a complaint against the pest control company Orkin for unilaterally raising customers' fees in violation of a term in those customers' contracts.[202] The administrative law judge hearing the case found for the agency, and Orkin appealed.[203] The appellate court affirmed the finding that unilaterally amending hundreds of thousands of contracts was an unfair practice.[204] While this action involved a price term (not a privacy term), it could provide grounds for the agency to take action against oppressive unilateral amendments.

Based on these examples, it would seem that the FTC could do its part to police problematic one-sided changes in the ToS and privacy policies of health apps. In fact, agency leaders have expressed interest in taking a more significant role in protecting consumer privacy.[205] But presently, the FTC may lack the ability to actually intervene in a meaningful way. To start, the prohibitions on unfair acts, in practice, are relatively thin.[206] Agency actions in this area typically consist of reviewing privacy policies and other representations and sometimes going after repeat offenders.[207] This limited activity could be the result of underinvestment in the agency itself. While the FTC may want to take more action on consumer privacy, staffing and resource shortages notoriously hamstring its ability to regulate effectively.[208]

b. State Data Protection Legislation

States also have statutes that protect consumer privacy. All fifty have at least one law governing breach notification for data collected online[209] and other regulations of health privacy.[210] For example, the

202 Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1359 (11th Cir. 1988).

203 *Id.*

204 *Id.* at 1368.

205 Rebecca Kelly Slaughter, Comm'r, Fed. Trade Comm'n, The FTC's Approach to Consumer Privacy 2 (Apr. 10, 2019) [hereinafter *Remarks of Rebecca Kelly Slaughter*].

206 Terry, *supra* note 144, at 95.

207 *Id.*

208 *See* Wagner, *supra* note 25, at 108; *Remarks of Rebecca Kelly Slaughter*, *supra* note 201, at 4 (stating "the single biggest change that would help the FTC in its role of enforcer of data privacy laws right now, would be an increase to our resources"); *see also* Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law*, BROOKINGS: TECHTANK (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/ [https://perma.cc/8THN-K8TA].

209 Geoff Scott, *Internet Privacy Laws in the US: A Guide to All 50 States*, TERMLY (Sept. 10, 2018), https://termly.io/resources/articles/privacy-laws-in-the-us/ [https://perma.cc/2UY8-9DU3].

210 Tovino, *supra* note 146, at 190–206.

recently enacted California Consumer Privacy Act (CCPA) gives consumers privacy rights in their "personal information."[211] Although not explicitly covering health-related data, the statute's definition of personal information may be broad enough to capture at least some data collected by health apps.[212] The statute provides Californians with a variety of rights related to their consumer data, including the right to be informed regarding data use and collection,[213] the right to notice of additional collection or use,[214] the right to have their information deleted,[215] the right to know of any data sales or disclosures,[216] the right to opt out of those sales,[217] the right to access their information,[218] and the right to equal services should they choose to exercise any of those preceding rights.[219] Practically speaking, many of these rights require action on the part of the user. For example, a consumer must *request* that the company disclose whether it sells the data of its users. These disclosures are not automatic.

Moreover, the CCPA's private right of action allows consumers to sue companies for both damages and injunctive relief if a company compromises its users' data after failing to take reasonable measures to protect it.[220] The statute is explicit that the ability to sue does not extend to other violations of the law.[221] In addition to this limited cause of action, the California Attorney General (AG) can bring enforcement actions.[222] In many cases, state AG enforcement is the best, most efficient way to investigate and prosecute consumer rights violations, including violations involving health privacy. They may also have their downsides. AG cases tend to prioritize large groups over individuals, and cases take considerable time to resolve, further harming individuals in the present in favor of protecting future

211 California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100(a) (West 2020), *amended by* California Privacy Rights Act of 2020, Proposition 24 (codified at CAL. CIV. CODE § 1798.100–.199.100) (effective Jan. 1, 2023). Notably, the statute applies only to companies that have gross annual revenues over $25 million, buy or sell the data of 50,000 or more consumers or households, or that earn more than half of their annual revenue from data selling. *Id.* § 1798.140(o)(1) (becoming 100,000 or more consumers or households in 2023).

212 *See id.* § 1798.140(o)(1).

213 *Id.* § 1798.100(b).

214 *See id.* § 1798.100.

215 *Id.* § 1798.105(a).

216 *Id.* § 1798.115(a).

217 *Id.* § 1798.120(a).

218 *Id.* § 1798.110.

219 *Id.* § 1798.125(a)(1).

220 *Id.* § 1798.150(a).

221 *Id.* § 1798.150(c).

222 *Id.* § 1798.155(b) (evolving into § 1798.199.90 effective 2023 while § 155 will cover administrative enforcement by the California Privacy Protection Agency).

rights.[223] Though we support AG action, we believe individual private rights of action are also necessary.

The CCPA has spurred similar efforts in other states, although their success has been somewhat limited.[224] Both Maine and Nevada have recently passed their own consumer data privacy laws.[225] Maine's statute, An Act to Protect the Privacy of Online Customer Information, prohibits "broadband Internet access service[s]" from disclosing, selling, or accessing "customer personal information" without consent.[226] It also requires covered entities to take reasonable steps to safeguard their users' data and to provide customers with notice of their rights and the providers' obligations under the act.[227] Unlike the CCPA, Maine's act explicitly covers "[t]he customer's health information."[228] However, the statute does not give consumers a clear private right of action.[229]

Nevada's law is more limited in scope than the CCPA and prohibits websites and offerors of online services from selling certain user data if the consumer requests them not to. As in California, the definition of "covered information" does not explicitly cover health-related data.[230] The consumer herself must actively opt out of any potential data sale by submitting a "verified request" to the company.[231] Congress also recently considered federal protections for consumer privacy.[232] Like Maine, Nevada does not provide for a private right of action.[233]

---

223 Stacey A. Tovino, *A Timely Right to Privacy*, 104 IOWA L. REV. 1361, 1382 (2019). Of course, even private enforcement favors large groups, considering the proliferation of class actions and multidistrict litigation. *See generally* D. Theodore Rave, *When Peace Is Not the Goal of a Class Action Settlement*, 50 GA. L. REV. 475 (2016).

224 Joseph J. Lazzarotti, Jason C. Gavejian, & Maya Atrakchi, *Maine and Nevada Sign into Law Consumer Privacy Laws*, JACKSON LEWIS (July 3, 2019), https://www.workplaceprivacyreport.com/2019/07/articles/california-consumer-privacy-act/maine-and-nevada-sign-into-law-consumer-privacy-laws/ [https://perma.cc/W6R4-4RU6].

225 *Id.*

226 ME. STAT. tit. 35-A, § 9301 (2019).

227 *Id.*

228 *Id.* § 9301(1)(C)(2)(e).

229 Peter J. Guffin & Kyle M. Noonan, *Maine's New Internet Privacy Law: What You Need to Know*, NAT'L L. REV. (June 14, 2019), https://www.natlawreview.com/article/maine-s-new-internet-privacy-law-what-you-need-to-know [https://perma.cc/7JRF-M3KX].

230 NEV. REV. STAT. § 603A.320 (2019).

231 *Id.* § 603A.345.

232 Christian Fjeld, Christopher Harvie & Cynthia J. Larose, *Congressional Privacy Action – Part 1: The Senate*, NAT'L L. REV. (Jan. 28, 2020), https://www.natlawreview.com/article/congressional-privacy-action-part-1-senate [https://perma.cc/G7QQ-KCYU].

233 NEV. REV. STAT. § 603A.360 (2019) ("The provisions of NRS 603A.300 to 603A.360, inclusive, do not establish a private right of action against an operator.").

Thus, consumer protections could offer some safeguards against unfavorable unilateral amendments in digital health tech. On the federal side, the FTC has shown a willingness to both protect the privacy of health app users and to police one-sided changes. Sadly, the agency in its current state may not have the bandwidth to serve as an effective consumer watchdog. Likewise, state protections may be insufficient as well. First, state laws apply to only a subset of Americans, leaving companies subject to multiple—perhaps conflicting—standards and the residents of other places vulnerable. Second, those statutes, which often do include private rights of action, may not offer individual consumers meaningful relief. More widespread solutions are therefore necessary to address the potential for one-sided changes in digital health tech and to provide consumers with the protections they need.

B. Critiques of Unilateral Amendments

As explained above, consumers who wish to challenge unfavorable one-sided changes have very few legal protections at their disposal. Despite their enforceability, unilateral amendment clauses are no strangers to criticism. Scholars have long argued that these provisions are fundamentally at odds with core principles of contract law and leave consumers vulnerable. In this Section, we outline these critiques of one-sided changes and argue that unilateral amendments—while problematic as a general matter—are particularly dangerous in the context of digital health tech.

1. Generally

To begin, the very idea of one-sided changes conflicts with some of the very basic principles of contract law. Every first-year law student learns that both forming and *modifying* a contract requires the parties' mutual assent.[234] Certainly, at least some courts have upheld this principle in recent years.[235] Yet, as explained above, courts are often

234 *See, e.g.*, ATACS Corp. v. Trans World Commc'ns, Inc., 155 F.3d 659, 666 (3d Cir. 1998) (quoting 1 SAMUEL WILLISTON, A TREATISE ON THE LAW OF CONTRACTS § 23 (Walter H.E. Jaeger ed., 3d ed. 1957)) (citing RESTATEMENT (SECOND) OF CONTRACTS § 22 (AM. L. INST. 1981)).

235 *See, e.g.*, Bd. of Trustees, Sheet Metal Workers' Nat'l Pension Fund v. Four-C-Aire, Inc., No. 16-CV-1613, 2017 WL 1479425, at *9 (E.D. Va. Apr. 21, 2017) (noting "the inoffensive rule that generally, 'a party to a contract does not have a right to unilaterally modify the contract'" because of "the value ascribed to contracts in our society" (first quoting Expo Props., LLC v. Experient, Inc., No. 14-688, 2016 WL 3997290, at *7 (D. Md. July 26, 2016); and then quoting Balt. Tchr.'s Union v. Mayor of Baltimore, 6 F.3d 1012, 1016 (4th Cir. 1993))), *rev'd and remanded*, 929 F.3d 135 (4th Cir. 2019).

more than willing to uphold unilateral amendment clauses. Perhaps enforcing one-sided changes is just part of the evolution of modern, boilerplate contracts, which itself contradicts the notion that people entering into contracts dicker over terms and bargain for things they value.[236] But apart from this theoretical disconnect, one-sided changes also raise several practical concerns that undermine fair and efficient contracting.

a. Suboptimal Consumer Decisionmaking

First, people are often not rational actors and will, as a result, make suboptimal decisions. There is an element of a bait and switch to one-sided changes: the company attracts customers with favorable terms, only to change those provisions unilaterally after the contract takes effect. Consumers entering into contracts may not anticipate those changes, even with a unilateral amendment clause.[237] Moreover, they may not appreciate the risk that companies will change contracts in a manner that harms individual consumers.[238] Even if consumers recognized the risk of changes to the contract in the abstract, assessing how likely an adverse change sometime in the future might be would be extremely difficult.

Of course, one might respond that consumers should demand contracts without unilateral amendment clauses, or at the very least, the informed minority of sophisticated consumers should do so. The informed minority theory, however, does not assume that informed consumers are completely rational. So, even informed consumers might neglect terms that are not initially salient to them, such as unilateral amendment provisions. Instead, they focus on terms that are immediately and concretely important, such as privacy terms.

A company's right to make unilateral changes is, therefore, the quintessential example of a contingent, long-term provision that consumers with bounded rationality will underweigh in importance.[239] In fact, unilateral amendments may actually discourage sophisticated consumers from signing up in the first place, thus undermining the potentially mitigating effects of the informed minority.[240]

---

236 *See* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 15 (2013).

237 *Cf.* Oren Bar-Gill & Omri Ben-Shahar, *Exit from Contract*, 6 J. LEGAL ANALYSIS 151, 154 (2014).

238 Bar-Gill & Davis, *supra* note 177*; see also* Hoffman & Wilkinson-Ryan, *supra* note 20, at 398–99 (noting that reforms to unilateral amendment laws "are motivated by the sense that unilateral modifications are unlikely to be welfare maximizing").

239 Oren Bar-Gill, *Seduction by Plastic*, 98 NW. U. L. REV. 1373, 1376 (2004).

240 Jake Linford, *Unilateral Reordering in the Reel World*, 88 WASH. L. REV. 1395, 1419 (2013); *see also* Bar-Gill & Davis, *supra* note 177, at 6.

b. Incomplete Risk Information

Additionally, research shows that people generally have trouble evaluating privacy policies because the policies are too complicated, contain too much information, and prey on systematic cognitive errors consumers make.[241] Adding the possibility of unilateral amendments to the calculus further compounds consumers' mistaken assessments. Unilateral amendments present a new level of uncertainty for users.

Even if a consumer is able to understand the existing terms and make a decision about the value of that exchange, the possibility of one-sided changes will complicate the equation. The result is possible pricing errors. Theoretically, every term in a contract has an associated price value. When a company changes a term to its own benefit, contract theory predicts that it would compensate consumers. For instance, if a company's privacy policy changed to allow it to gather and sell more consumer data, the company should compensate its users for that potentially lucrative new term. But companies generally do not remunerate consumers for changed terms even if the modification benefits the company.[242] Almost always, these changes hurt consumers without compensating them.

Of course, one might argue that an informed consumer who has read the terms will be aware of the potential for one-sided changes and will factor that possibility into what she is willing to pay for the contract. That theory fails to play out in reality. When entering contracts with unilateral amendment clauses, consumers must make assumptions about the array of possible changes and the cost at which those modifications would theoretically be acceptable to them in the future. This process requires valuing guesses about not only what a company may do but how a person may feel. The compensation consumers should demand for companies' power to unilaterally amend is extremely difficult to assess at the start of a transaction.[243] Thus, when the thing a consumer is bargaining for is privacy, allowing one-sided changes can be even more harmful to consumers who will have difficulty accurately assessing risk.

241 Kristoffer Bergram, Tony Gjerlufsen, Paul Maingot, Valéry Bezençon & Adrian Holzer, *Digital Nudges for Privacy Awareness: From Consent To Informed Consent?*, *in* EUROPEAN CONFERENCE ON INFORMATION SYSTEMS, RESEARCH PAPERS, June 2020, at 1, 4 (2020); *see also* Leah R. Fowler, Charlotte Gillard & Stephanie R. Morain, *Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications*, 21 HEALTH PROMOTION PRAC. 679, 681 (2020); Ali Sunyaev, Tobias Dehling, Patrick L. Taylor & Kenneth D. Mandl, *Availability and Quality of Mobile Health App Privacy Policies*, 22 J. AM. MED. INFORMATICS ASS'N e28, e31 (2015).

242 Horton, *supra* note 20, at 651.

243 Linford, *supra* note 240, at 1417.

c. Switching Costs

Unilateral amendment clauses also prevent the market from functioning correctly because these transactions often involve high switching costs. Recall that courts typically view continued use as consent to new terms. Thus, once a one-sided change takes effect, consumers who do not wish to agree to those modifications must stop using the product or service.

To find new services, consumers would incur substantial switching costs. Not only does changing services require "time, effort, and sometimes money," inertia and status quo bias—our tendencies to keep what we have—make switching to a new product unlikely even if it is a rational choice.[244] Already having a product in the first place may be sufficient justification to keep using that product, even after a disadvantageous modification.[245] This reality is not lost on sellers who may seek to lock consumers in.[246] The result is that companies can change their terms with little or no market pressure to consider the preferences of their users.[247]

d. Contract Distancing and Lack of Notice

Moreover, even users who initially shop for desirable terms might not be able to keep up with a company's one-sided changes once the contract takes effect. Contract distancing, "the lack of proximity between consumers, contract terms, and the contract formation process," makes it unlikely that users will ever see unilateral amendments.[248] And generally speaking, consumers are less likely to scrutinize their trading partners' behavior after the parties have formed an initial contract.[249] Thus, a person who took the time to select a product based on its terms may not continue to monitor the contract after the fact. And recall from Part I that many companies do not notify their users of modified terms and instead charge the consumers themselves with staying up to date. Keeping abreast of those changes can prove unduly costly.[250] People, many of whom struggle to read the initial terms and privacy policies, cannot be

244 *See* Bar-Gill & Ben-Shahar, *supra* note 237, at 153 n.1; *see also* RADIN, *supra* note 236, at 27.

245 Linford, *supra* note 240, at 1415.

246 *See* Bar-Gill & Ben Shahar, *supra* note 237, at 153 n.1.

247 *See* Adam J. Levitin, *Rate-Jacking: Risk-Based & Opportunistic Pricing in Credit Cards*, 2011 UTAH L. REV. 339, 363.

248 Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 843, 882 (2016).

249 Hoffman & Wilkinson-Ryan, *supra* note 20, at 399.

250 Linford, *supra* note 240, at 1417.

reasonably expected to monitor and review modifications to their existing contracts,[251] despite the duty to read changes.[252]

2. In Digital Health Tech

While health app consumers are vulnerable for all the reasons explained above, unilateral amendments raise specific concerns in digital health tech.

a. Incorrect Assumptions About Medical Privacy

First, anyone who has seen a doctor in the United States has probably signed a HIPAA privacy statement.[253] As a result, many Americans have at least some notion of health privacy. Unfortunately, HIPAA is profoundly and widely misunderstood, with the general public notoriously believing that its protections are far more expansive than they truly are.[254] Given the widespread belief that HIPAA protects individuals from sharing health information with *anyone*, it is reasonable that many also mistakenly believe it applies to health apps. So, it would be logical to infer that if HIPAA protects your blood pressure data at the doctor's office, it will likewise apply to that very same data logged at home with a digital blood pressure cuff. Of course, that is often not the case. Regardless, health app users may nonetheless have higher—although misguided—baseline expectations regarding the privacy of their health-related data.

Complicating matters further, certain companies may actually cultivate this confusion using their branding. Some health apps outwardly present themselves as healthcare providers—through pictures, titles, or vague characterizations in their marketing

251 *See* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 73 (2014).

252 KIM, *supra* note 187, at 65–67.

253 45 C.F.R § 164.520 (2020).

254 Consider the backlash to mask requirements during the pandemic. Opponents to these requirements claimed, among other legal rights, that HIPAA prevents anyone—companies, the government, other private citizens—from asking why a person is not wearing a mask. Lois Shepherd, *COVID-19 State Mask Mandates Can't Be Avoided Using HIPAA or Constitutional 'Exemptions,'* NBCNEWS: THINK (Aug. 11, 2020), https://www.nbcnews.com/think/opinion/covid-19-state-mask-mandates-can-t-be-avoided-using-ncna1236342 [https://perma.cc/F9YF-ZTX7]. They incorrectly reasoned that asking a person why she could not wear a mask would require disclosure of protected health information. This misapplication of HIPAA was so common during the pandemic that multiple news outlets ran interviews with legal experts. Camille Caldera, *Fact Check: No Mask? You Can Ask Why – It Isn't Against HIPAA or the Fourth or Fifth Amendments*, LAS CRUCES SUN NEWS (July 20, 2020), https://www.lcsun-news.com/story/news/factcheck/2020/07/19/fact-check-asking-face-masks-wont-violate-hipaa-4th-amendment/5430339002/ [https://perma.cc/T8AR-A425].

materials—while simultaneously disclaiming that status in the fine print to avoid regulation.[255] That branding may further lull consumers into a false sense of security.

Consumers' misconceptions regarding health privacy could exacerbate their vulnerability to one-sided changes. Imagine that someone shopping for a period-tracking app browses several options and selects one based on its commitments to privacy and data security, bolstered by the assurances of company officials wearing white medical coats featured on the website. That person might reasonably believe based on her experience that the company would keep its promises to her. Despite her willingness to initially shop for terms, she might then be less likely than the average consumer to regularly check for updates to the ToS and privacy policy because of her belief that medical privacy laws will protect her.

b. Heightened Switching Costs

Switching costs may also be higher in digital health tech than in other contexts. For non-health apps, stopping use may mean walking away from a hard-earned high score in a gaming app.[256] By contrast, if users leave their current health app, they might forgo years of valuable health-related data that could inform important life choices.

To start, it takes considerable time and effort to meticulously monitor and track such detailed data over months and even years. Thus, the switching costs here are greater than with other types of apps. Additionally, the lack of interoperability between different health apps freezes customers into relationships, making an exit extremely costly. Therefore, users may be reluctant to leave that data on the table.

Furthermore, the products themselves are not fungible. For example, with period trackers, the value of predictive information,

255 Kit Huckvale, John Torous & Mark E. Larsen, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, 2 JAMA NETWORK OPEN, Apr. 2019, at 1, 2. The FTC could theoretically intervene in cases in which the advertising crosses acceptable boundaries, such as those of AcneApp and Acne Pwner, which made health-related claims without evidence. *"Acne Cure" Mobile App Marketers Will Drop Baseless Claims Under FTC Settlements*, FED. TRADE COMM'N (Sept. 8, 2011), https://www.ftc.gov/news-events/press-releases/2011/09/acne-cure-mobile-app-marketers-will-drop-baseless-claims-under [https://perma.cc/S99G-LE5T]. However, there have not been enforcement actions for advertising materials using medical imagery—like a caduceus—or for having a "chief medical officer." *See, e.g.*, Christina Farr, *Online Therapy Start-up Talkspace Hires a Chief Medical Officer from UnitedHealth*, CNBC (Apr. 11, 2018), https://www.cnbc.com/2018/04/11/talkspace-hires-a-chief-medical-officer-ahead-of-potential-ipo.html [https://perma.cc/8E7U-SQRY].

256 Oren Bar-Gill and Omri Ben-Shahar have argued that exit is a powerful consumer protection tool. Bar-Gill & Ben-Shahar, *supra* note 237, at 152.

such as dates of menstruation, ovulation, or onset and duration of premenstrual syndrome (PMS) symptoms, is only realized over time. Natural Cycles specifically notes that it takes several cycles for the algorithm to "get to know you" in a way that allows it to predict ovulation.[257] Apps like Flo advertise that the more information users can add about their cycles, the more accurate their predictions will become over time.[258] Starting over with a new service will mean less reliable predictions and recommendations, at least in the short term.

C. A Brief Defense of Unilateral Amendments

Despite the many arguments presented in this Article against them, the ability of companies to make one-sided changes is not wholly without value. As a practical matter, unilateral amendment clauses reflect the reality of contracting in the digital marketplace. For each app, thousands of users download the product. Bilateral amendments, in which both parties participate in the negotiation, could be impractical given the sheer volume of consumers and their different preferences. Unilateral amendments, by contrast, are much faster, lower cost, and ensure uniformity across users. This efficiency is one of the strongest arguments in favor of unilateral amendments.

And, of course, unilateral amendments are not uniformly nefarious. While it is easy to envision changes intended to exploit users and profit from their data, one could also predict other, more benevolent kinds of modifications. For example, changes to contract terms might be in response to public outcry,[259] legislation,[260] or recent judicial decisions invalidating existing terms.[261] Thus, not all one-sided changes will hurt consumers. Some may actually benefit them. Particularly in fast-paced industries such as digital health tech, the flexibility of unilateral amendments allows companies to act quickly to improve their services, perhaps by incorporating scientific breakthroughs or by updating their technology, ultimately delivering a better product to their users. We do not want to hamper the ability

257 *How Long Will It Take the App To Get To Know My Cycle?*, NC: CYCLERPEDIA, https://help.naturalcycles.com/hc/en-us/articles/360003313193-How-long-will-it-take-the-app-to-get-to-know-my-cycle [https://perma.cc/LRS5-Z9DV].

258 Flo's materials thus implore users to be as detailed as possible: "Your mood swings, activities, physical indications — try to log as many of these as you can. The more data our AI has to process and analyze, the higher Flo app accuracy will become. Don't be afraid to make Flo work harder for you — it can handle it :)" *How Accurate Is the Flo App? All About Flo Accuracy*, FLO, https://flo.health/faq/accuracy [https://perma.cc/S9DQ-EAZM].

259 *Supra* notes 110–14 and accompanying text.

260 *Supra* note 111 and accompanying text.

261 Horton, *supra* note 20, at 645.

of companies to make these kinds of consumer-friendly, socially beneficial changes.

* * *

Health app users currently have very little recourse to challenge unilateral amendments to ToS and privacy policies. Traditional health law and regulations generally do not apply to digital health tech, and both contract and consumer law generally tolerate one-sided changes, despite their potentially negative effects on users. Not surprisingly then, scholars have criticized unilateral amendment provisions as unfair to consumers. While all of those standard critiques also apply to health apps, we maintain that unilateral amendments in digital health tech raise special concerns. Of course, we do not want to get rid of the good with the bad. One-sided changes—under the right circumstances—can have real benefits for consumers, including health app users. We now turn to how law- and policymakers could better protect consumers of digital health tech while still allowing companies to make socially beneficial unilateral amendments.

III. IMPROVING DIGITAL HEALTH TECH

Unilateral amendment clauses in ToS and privacy policies, though common, disrupt the market for privacy in digital health tech and leave consumers vulnerable. Because one-sided changes can at times benefit consumers, we do not advocate barring them completely. Instead, we simply want to give consumers more protection against potentially unfavorable unilateral amendments. But striking the appropriate balance is no easy task. Part III turns to potential legislative, regulatory, and judicial solutions.

We center our recommendations on contract and consumer law. While expanding HIPAA or FDA oversight to cover health apps might seem like a promising strategy, it would perpetuate the data-protection siloing that already plagues the United States.[262] We, therefore, advocate for improved consumer data protections across the board and, as a second-best option, judicial interventions. Certainly, our focus has been digital health tech, but the issues that we have identified extend far beyond this particular market. Plenty of non-health apps collect highly personal information. Navigation apps, like Waze and Google Maps, track and store highly personal and identifiable geolocation data.[263] Budgeting apps, like NerdWallet and Spending

262 *See* Terry, *supra* note 144, at 95.

263 Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, BUS. L. TODAY (Mar. 25, 2019), https://businesslawtoday.org/2019/03/power-place-geolocation-

Tracker, collect and analyze personal financial data, including income, expenses, and debt.[264] And dating apps, like Grindr and Bumble, not only document their users' preferences in a sexual or romantic partner but also their drug use, contact information, photographs, and sometimes disease history.[265] Simply, extending health privacy laws to digital health tech would leave these other consumers—and their intimate, identifiable data—at risk. Hence, the problems that we identify are, at their core, issues for contract and consumer law, not health law.

A. Legislative Solutions

As noted in the preceding Part, Americans lack clear, unified protections for consumer data, as well as the ability to challenge harmful one-sided changes. Users in other countries have both greater control over their data and stronger protections against unfavorable unilateral amendments. Take, for example, Europe's General Data Protection Regulation (GDPR), which burdens app developers with obtaining clear permission before collecting or sharing intimate user data.[266] The statute contains a robust definition of consent, which must be "freely given, specific, informed and unambiguous."[267] By contrast, consumer data in the United States is underregulated, and what protections do exist remain fragmented.[268]

Moreover, outside of the United States, many of the unilateral amendment provisions described in Part I would be unenforceable. For example, including a term that would allow one party to make sweeping changes to the contract without the consent of the other party would likely violate the United Kingdom's Competition and

---

tracking-privacy/ [https://perma.cc/6KAP-BCRE]; *Google Maps*, APPLE, https://apps.apple.com/us/app/google-maps-transit-food/id585027354 [https://perma.cc/V536-HHY8]; WAZE, https://www.waze.com [https://perma.cc/D5GS-XSX5].

264 Steven Abrams, *The Hidden Cost of Free Financial Apps*, US NEWS (Nov. 30, 2018), https://money.usnews.com/money/blogs/my-money/articles/the-hidden-cost-of-free-financial-apps [https://perma.cc/AFT6-Z239]; NERDWALLET, https://www.nerdwallet.com [https://perma.cc/B8YA-BW7W]; *Spending Tracker*, APPLE, https://apps.apple.com/us/app/spending-tracker/id548615579 [https://perma.cc/HRP8-PNWX].

265 Conor Ferguson, Andrew W. Lehren, Keir Simmons & Didi Martinez, *Dating Apps Like Grindr Could Pose a National Security Risk, Experts Warn*, NBC NEWS (Jan. 14, 2020), https://www.nbcnews.com/tech/security/dating-apps-grindr-could-pose-national-security-risk-experts-warn-n1115321 [https://perma.cc/F7UR-JVWG].

266 Commission Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1.

267 *Id.* art. 4(11).

268 Terry, *supra* note 144, at 97–98.

Markets Authority Guidance on Unfair Contract Terms.[269] Unlike the broad and inclusive safeguards in other countries, consumer protections in the United States differ across industries. Congress has limited one-sided changes in the financial sector[270] but not in other areas, yet again leaving Americans with a splintered system.

We therefore propose enacting broad, "domain agnostic[]"[271] legislation that would both give consumers more robust rights in their data and require companies to obtain consent for making material changes to their ToS or privacy policies. Unified, federal statutory protections—perhaps with a role for the FTC to issue industry-specific rules—is one way to protect consumers from potentially harmful one-sided changes.[272]

1. Federal Data Protection Legislation

Certainly, we are not the first to advocate for federal consumer privacy legislation. A number of scholars[273] and the FTC[274] itself have already made several thoughtful proposals regarding how to better protect Americans' consumer data. And Congress itself has shown an interest in acting on these issues. Before the pandemic hit in early 2020, members of Congress had introduced three bills related to consumer privacy: two in the Senate and one in the House.[275] Although differing in key ways,[276] the proposed legislation emphasized similar principles as the GDPR, including requiring transparency in

---

269 ANDELKA M. PHILLIPS, BUYING YOUR SELF ON THE INTERNET: WRAP CONTRACTS AND PERSONAL GENOMICS 164–219 (2019); *see* Andelka M. Phillips, *Only a Click Away – DTC Genetics for Ancestry, Health, Love . . . and More: A View of the Business and Regulatory Landscape*, 8 APPLIED & TRANSLATIONAL GENOMICS 16, 21 (2016).

270 Generally speaking, lenders who offer open-ended home equity loans cannot change the price of the loan without consent. Eric Andrew Horwitz, Note, *An Analysis of Change-of-Terms Provisions as Used in Consumer Service Contracts of Adhesion*, 15 U. MIA. BUS. L. REV. 75, 85–86 (2006).

271 We borrow this phrasing from Nicolas P. Terry. Terry, *supra* note 144, at 98.

272 *See* Rich, *supra* note 208.

273 *See, e.g.*, Joshua D. Blackman, *A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector*, 9 SANTA CLARA COMPUT. & HIGH-TECH. L.J. 431 (1993); Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199 (1993); Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*, 10 CYBARIS INTELL. PROP. L. REV. 1 (2019); Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413 (2013); Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and* the Right [Approach] to Privacy, 80 ANTITRUST L.J. 121 (2015).

274 Rich, *supra* note 208.

275 Fjeld, Harvie & Larose, *supra* note 232.

276 For example, the Republican bill is narrower in scope and more lenient about compliance than its Democratic counterpart. *Id.*

privacy policies and giving consumers better control over their data.[277] Given that much ink has been spilled considering how to best legislate in this area, we do not focus our attention here on the general provisions of a federal data protection statute. Instead, we outline how we think such a law could best safeguard users from damaging, one-sided changes.

Some data subjects are already entitled to notice of changes that could affect their rights. For example, under HIPAA, patients have a right to notice of the privacy practices that govern their protected health information.[278] The law requires that the notice be in plain language and that it contain both descriptions and examples.[279] Covered entities must promptly revise and redistribute their privacy notices in the event of material changes that would affect a variety of areas, including the uses or disclosures of the data, the rights of the data subjects, and the covered entities' legal duties.[280] Furthermore, unless required by law, those changes cannot take effect before the notice.[281] While we would like our proposals to affect all consumers—not just health app users—lawmakers could nonetheless turn to HIPAA's notice requirement or similar kinds of protections as a reference point for how to best inform consumers.

Importantly, companies would not have to provide notice of *all* unilateral amendments, only those that are material to users. The law could thus permit companies to make procedural or technical changes without consent from consumers. In fact, a statute could even enable companies to make unilateral amendments that clearly benefit users, say by improving the accuracy of the app or increasing a person's rights in her data. In February 2021, Digital Lab at Consumer Reports issued a Model State Privacy Act.[282] The model statute included a list of uses that would not require consent from the user.[283] These presumptively valid uses included debugging and repairing errors to improve functionality, internal research for product development and improvement purposes, activities to verify the quality or safety of the product or service, and efforts to enhance or upgrade the product or

277 The Democratic bill requires that entities have a publicly available privacy policy and requires consumer consent to make material changes. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 102(b), (d) (2019). The Republican bill also requires that entities have a publicly available privacy policy and requires notice of material changes. Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. § 4(a), (e) (2020).

278 45 C.F.R. § 164.520 (2020).

279 *Id.*

280 *See id.* § 164.520(b)(3) (describing the requirement for health plans).

281 *Id.*

282 JUSTIN BROOKMAN & MAUREEN MAHONEY, CONSUMER REPS., MODEL STATE PRIVACY ACT (2021).

283 *Id.* § 3(n).

service.[284] Likewise, under our proposal, unilateral amendments for these kinds of purposes would not require notice and consent. Companies could then freely change their ToS and privacy policies if the goal would be to improve the technology, to enhance consumer rights, or to comply with changing scientific or legal norms. Additionally, changes that are primarily ministerial would also be acceptable. Requiring notice and consent for only material changes would allow companies to unilaterally amend their terms without the burden of contacting users about neutral or beneficial changes.

For changes to material terms that could adversely impact consumers, companies would have to go about making changes the good old-fashioned way: by obtaining consent. Existing consumer privacy legislation offers definitions of consent that could serve as a template. Under the GDPR, users indicate their "freely given, specific, informed and unambiguous" consent "by a statement or by a clear affirmative action."[285] The amended CCPA described in Part II adopts a very similar definition.[286] It is also specific about what does *not* qualify as consent, including accepting general or broad terms that include unrelated information.[287] It further provides that "[h]overing over, muting, pausing, or closing a given piece of content does not constitute consent."[288] The amended CCPA also prevents companies from using "dark patterns," interfaces specifically designed to trick or mislead users,[289] to obtain consent.[290] We would adopt a similarly robust notion for consent when consumers agree to material changes.

Importantly, we argue that users who do not wish to agree to the new terms should keep their original agreements. Certain digital health tech companies already give users the ability to opt in and out of certain services, such as participating in research or being

284 *Id.*

285 Commission Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46 /EC, 2016 O.J. (L 119) 1, art. 4(11).

286

> 'Consent' means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose.

California Privacy Rights Act, CAL. CIV. CODE § 1798.140(h) (West 2020) (effective Jan. 1, 2023).

287 *Id.*

288 *Id.*

289 BROOKMAN & MAHONEY, *supra* note 282, at 1.

290 California Privacy Rights Act §§ 1798.140(h), (*l*) (effective Jan. 1, 2023).

searchable on a database of users. They could adopt similar kinds of options when making changes to material terms in the company's ToS or privacy policy. Allowing users to keep their old terms will address the issue of high switching costs described in Part II. No longer will consumers have to make the Hobson's choice of abandoning all of their data or agreeing to harmful new terms.

Enforcement of these legislative provisions could take a few different forms. A statute could empower the FTC to enforce the law, an option that we consider at greater length in the following Section. It could also allow the Attorney General to enforce the statute. Agency and AG enforcement both have their upsides. In particular, individual plaintiffs do not have to bear the potentially high cost of litigation. However, the FTC and U.S. Attorneys would have to be selective about which cases they take, and individuals will not get the opportunity for relief. We therefore advocate a multilayered enforcement approach that would pair administrative enforcement with a private right of action to empower individual consumers.[291] Lawmakers could make the failure to get consent for an unfavorable, material change actionable in and of itself. Consumers would not have to prove an accompanying physical, emotional, or financial harm.[292] The law could also include statutory damages to ensure both that users are properly compensated and that companies are sufficiently deterred.

2. Objections and Responses

All of that said, enacting sweeping consumer protection legislation is theoretically desirable but practically challenging. Comprehensive federal reform will give consumers the best protections yet is probably the most difficult to enact from a logistical perspective. The fact that members of Congress from both parties have recently proposed data privacy bills may make it seem like this issue would provide a promising opportunity for political consensus. Unfortunately, Congress has been considering this issue for years and with very little progress.[293]

Even if lawmakers could come to an agreement, the law may soon find itself obsolete. Drafting legislation is time consuming. By

---

291 Several consumer laws already use this public-private enforcement structure. For instance, the Texas Deceptive Trade Practices Act allows the Texas AG or private consumers to sue under the Act. *See* TEX. BUS. & COM. CODE ANN. §§ 17.46, 17.50 (West 2021).

292 *See* Cole v. Gene by Gene, Ltd., No. 14-CV-00004, 2017 WL 2838256, at *5 (D. Alaska June 30, 2017) (finding that the plaintiff had standing under *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016), even without a "tangible economic or physical harm").

293 *See* Matt Laslo, *Hey Congress, How's That Privacy Bill Coming Along?*, WIRED (Nov. 29, 2019), https://www.wired.com/story/congress-privacy-bill-copra/ [https://perma.cc/AF6W-F9XX].

contrast, the technology sector is notoriously fast paced. Once standards are set, it may be difficult to go back and make changes. What might represent the industry gold standard now might be antiquated and obsolete a few years later. While Congress could offer much needed clarity for consumers and companies alike, the same specificity and predictability that makes legislative interventions appealing also means that they may not age well.

B. Regulatory Solutions

As noted in Part II, the FTC currently has regulatory authority over consumer health apps and has expressed an interest in taking a more active role to ensure user privacy. Thus, another potential option would be to give the agency greater enforcement capabilities to police unfavorable one-sided changes to ToS or privacy policies.[294]

1. Increased Federal Trade Commission Oversight

An increased role for the FTC could take a few different forms. One possibility would be to charge the agency with both the interpretation and the enforcement of a federal data protection statute, like the one proposed above. For example, the statute could enable the FTC to issue rules or guidance[295] defining which kinds of terms are material and which types of changes implicate privacy or data security, as well as to bring complaints against violators. These documents could help guide health app developers in drafting as well as modifying their ToS and privacy policies. Providing uniform definitions for key terms and setting data security standards will help streamline consumer protections not only across digital health tech products but also other kinds of technologies. Moreover, the FTC could also weigh in on which kinds of unilateral amendments are acceptable, thus allowing companies to make changes that are neutral or beneficial. Thus, the agency could enact carefully drafted, detailed rules that both protect consumers and offer clear guidance to companies.

---

294 Terry, *supra* note 144, at 95 (describing the current FTC prohibitions as "thin").

295 The scope of the FTC's authority could vary depending on the content of the statute. Take the federal privacy bills described in the preceding Section. While both Senate bills would empower the FTC to enforce the law, the Republican bill would only give the agency rulemaking authority with respect to certain provisions and the ability to issue nonbinding guidance. Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. §§ 2(14)(K), 3(c)(6)(E), 5(i) (2020). By contrast, the Democratic bill charges the FTC with general rulemaking authority. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 110(h) (2019).

Absent a broad federal data protection statute, the FTC could play a larger role in safeguarding consumers. Ideally, Congress could allocate more resources to the agency to improve its effectiveness as a consumer watchdog. Increasing funding for the FTC might be more politically feasible at the present moment than enacting sweeping legislation.[296] FTC enforcement may actually be preferable to legislation because the agency can respond more deftly to evolving technologies.[297] There are also things the agency could do itself even without the support of Congress or additional resources. Jessica Rich, a former director of consumer protection at the FTC and a manager of the agency's privacy program, has encouraged the FTC to act now to improve its reach and its effectiveness.[298] Her suggestions include adding a new "Bureau of Data Protection" to the agency's two primary bureaus to streamline its efforts to address threats to consumer privacy and data security, issuing a "Commission Policy Statement on Consumer Harm" to both educate consumers and lay the groundwork for future enforcement actions, and convening a "Public Workshop on Privacy 'Third Rails'" to further policy discussion and develop potential solutions.[299]

An invigorated FTC could better protect consumers in at least two ways: through enforcement and through education. The agency could use its discretion regarding when unilateral amendments are harmful and when they are acceptable. It could also ensure that the representations that companies make about their privacy in their advertisements do not mislead consumers following a one-sided change.[300] In addition to enforcement actions, the FTC could take greater steps to educate both users and app developers. The FTC already makes efforts to promote consumer awareness and to advise companies about their privacy practices.[301] On the user side, the agency could educate the

296 *See Congress Reflects on the Long Path Ahead in Federal Data Privacy Legislation*, ACA INT'L (Sept. 23, 2020), https://www.acainternational.org/news/congress-reflects-on-the-long-path-ahead-in-federal-data-privacy-legislation [https://perma.cc/9A3H-D2JK]; Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, But Not Without Help from Congress*, BROOKINGS: TECHTANK (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/89WG-BLBH].

297 Wagner, *supra* note 25, at 103–04.

298 Jessica Rich, *Five Reforms the FTC Can Undertake Now to Strengthen the Agency*, BROOKINGS: TECHTANK (Mar. 1, 2021), https://www.brookings.edu/blog/techtank/2021/03/01/five-reforms-the-ftc-can-undertake-now-to-strengthen-the-agency/ [https://perma.cc/PV3U-X3X2].

299 *Id.*

300 For the discussion of the role of advertising in the market for privacy and how one-sided changes can lead to market failures, see *supra* Section I.B.

301 *See* Christi J. Guerrini, Jennifer K. Wagner, Sarah C. Nelson, Gail H. Javitt & Amy L. McGuire, *Who's on Third? Regulation of Third-Party Genetic Interpretation Services*, 22 GENETICS

public about their rights and help them to better understand how apps gather and store their data, thus allowing consumers to make more informed decisions. It could also explain the possibility of one-sided changes so that users selecting a product will be more aware of unilateral amendment clauses. With a newfound knowledge of these provisions, a person might select a health app that promises to notify its users of its updates, as opposed to an app that requires its users to regularly check its website for changes. In keeping with the informed minority hypothesis, even a subset of educated consumers could pressure app developers to create more transparent, user-friendly terms for making one-sided changes. On the industry side, the FTC could guide digital health tech companies and other types of app developers regarding best practices for privacy and data security and counsel them about which kinds of unilateral amendments are appropriate and which kinds of changes require notice and consent.

Thus, a more active FTC could have real benefits for consumers but without completely eliminating the possibility of unilateral changes.

2. Objections and Responses

While the FTC might offer a more politically palatable, adaptable alternative to a federal consumer data protection statute, it will not give consumers ready access to relief. Agency enforcement without related legislation would not include a private right of action. Users would therefore be unable to personally recover from the harms that resulted from an unfavorable one-sided change. And—while sidestepping the legislative process may be practically appealing—Americans will likely be less aware of a regulatory solution than a legislative one. Unfortunately, people pay little attention to FTC privacy actions.[302] Thus, the FTC will have to invest significant resources if it wishes to educate and empower the public in the ways described above.

In sum, increased FTC oversight has its clear advantages. It may be easier to implement than federal legislation, and the agency's expertise will benefit both companies and consumers alike. But agency enforcement may not be enough on its own, especially because it would not give individual users the opportunity for relief.

MED. 4, 9 (2020); *Mobile Health Apps Interactive Tool*, *supra* note 148; Wagner, *supra* note 25, at 108.

302 Solove & Hartzog, *supra* note 169, at 606.

C. Judicial Solutions

Legislative and regulatory solutions can offer comprehensive yet nuanced responses to the problems caused by unilateral amendments. In so doing, both require time and resources to take effect. Regardless, there is no reason why courts cannot act immediately to mitigate these harms.[303] Unlike those other options, judicial action can occur as soon as courts encounter unilateral amendment cases.[304] And it has the benefit of giving aggrieved users the opportunity to recover.

Part II argued that courts have not reliably protected consumers from abusive unilateral amendments through contract law, but they could. Contract law currently has at least one underexplored doctrinal tool that courts could use to police oppressive one-sided changes. Specifically, this Section argues that courts can and should embrace a more robust doctrine of good faith in these cases. Good faith is sufficiently fluid and capacious to adapt to the various circumstances that can arise involving unilateral amendments, allowing courts to differentiate between the changes that hurt consumers and the changes that help them. It is also a good fit with the health app context where one party—the consumer—is at the mercy of another party—the business with the ability to change the terms of the deal.

1. Enhanced Duty of Good Faith

Good faith is an excellent doctrinal resource for courts that want to police unilateral amendments because courts can adapt the doctrine as the situation requires. For more than fifty years, scholars have pointed out good faith's fluidity.[305] The classic statement of good faith's definition comes from its opposite. In *Kirke La Shelle Co. v. Paul Armstrong Co.*, the court defines bad faith as that "which will have the effect of destroying or injuring the right of the other party to receive the fruits of the contract."[306] While several other definitions exist, the one most helpful to consumers is the notion that good faith protects parties subject to the other sides' discretion.[307] Obligations of good faith exist outside of the common law of contracts, as well. For example, the Uniform Commercial Code (UCC) requires that buyers

303 Albert H. Choi & Geeyoung Min, *Contractarian Theory and Unilateral Bylaw Amendments*, 104 IOWA L. REV. 1, 41 (2018).

304 *Id.*

305 *See* Richard S. Wirtz, *Good Faith and the Morals of the Marketplace*, 36 QUINNIPIAC L. REV. 231, 232 (2018).

306 Kirke La Shelle Co. v. Paul Armstrong Co., 188 N.E. 163, 167 (N.Y. 1933); *see also* Steven J. Burton, *Breach of Contract and the Common Law Duty to Perform in Good Faith*, 94 HARV. L. REV. 369, 379–80 (1980).

307 *See* Burton, *supra* note 306, at 383–84.

entering into requirements contracts act in good faith.[308] In a requirements contract under the UCC, a seller promises to offer as much of a good as the buyer "requires," in exchange for being the exclusive supplier of that good.[309] The UCC states that buyers must determine the amount of goods they need in good faith.[310] In that instance, the seller is at the mercy of the buyer who, in the absence of a good faith requirement, could suddenly require more goods or no goods at all, depending on market conditions.

Unilateral amendment provisions give the health tech company discretion to change the terms of the contract with essentially no input from the consumer. Like the seller in the requirements contract, users are at the mercy of the health tech company here. The doctrine of good faith could set limits on health tech companies' use of that discretion. Health tech companies should not be able to use their discretion to destroy the consumers' right to "receive the fruits of the contract"[311]—that is, the protection of consumers' data from unexpected uses. Importantly, a heightened duty of good faith would not impede a company from making one-sided changes that were neutral or beneficial.

Courts have already invoked the duty of good faith related to unilateral amendments, so there is precedent on which to draw. While *Tompkins v. 23andMe, Inc.* rejected unconscionability, the court noted that a company with the power to make one-sided changes could only do so in good faith.[312] Good faith could thereby protect consumers from unreasonable modifications.

Furthermore, relying on good faith would also avoid some of the downsides of the other contract doctrines described in Part II. Recall that the doctrine of illusory promises renders the contract void. It is therefore of little use to parties who wish to enforce the contract. Health app users who want to challenge unfavorable one-sided changes do not want to invalidate the contract: they want to enforce the old terms. Under the doctrine of good faith, failing to act in good faith constitutes a breach. Thus, if a digital health tech company unilaterally amended its ToS or privacy policy in a way that harmed users, the users could challenge that change as in bad faith and therefore legally actionable while keeping the contract intact.

308 U.C.C. § 2-306 (AM. L. INST. & UNIF. L. COMM'N 2020). A requirements contract is when "the buyer binds himself to purchase all of his requirements from the seller in exchange for a promise from the seller to supply the buyer's needs." *Requirements Contracts Under the Uniform Commercial Code*, 102 U. PA. L. REV. 654, 654 (1954).

309 U.C.C. § 2-306 (AM. L. INST. & UNIF. L. COMM'N 2020).

310 *Id.*

311 *Kirke La Shelle Co.*, 188 N.E. at 167.

312 Tompkins v. 23andMe, Inc., 840 F.3d 1016, 1033 (9th Cir. 2016).

Similarly, unconscionability is usually a defense to breach, not grounds for recovery. Hence, much like with illusory promises, it is of little use to consumers in the context of unilateral amendments. But the doctrine of good faith provides a path to recovery. Additionally, a consumer arguing that a health tech company must only amend in good faith does not have to show that the consumer is necessarily the weaker party, just that the health tech company has the discretion to exercise power and control over the transaction.[313] Unconscionability is difficult to establish because of the rigorous requirements for establishing the defense.[314] Good faith, on the other hand, is always applicable, and courts have more latitude using it to prevent harmful amendments.

Summing up, the doctrine of good faith would allow consumers to sue for unfavorable one-sided changes without invalidating the underlying agreement. Also, good faith is sufficiently flexible to give companies the ability to make benign or helpful changes without the administrative burden of seeking user consent.

2. Objections and Responses

Several objections may arise to employing good faith in this context that are both practical and doctrinal in nature. On the practical side, contract law might not be the best vehicle for reform. Courts trying to change the law require cases to decide, and consumers may not sue over unilateral changes.[315] Moreover, litigation is an expensive, lengthy, and uncertain process, and remedies will be piecemeal and context dependent. And finally, many health app users may be subject to inescapable arbitration agreements. For all these reasons, legislative or regulatory solutions are arguably preferable.[316]

On one level, we agree that legislative or regulatory action is superior to judicial action. On the other, we believe that judges can still have a positive impact in this area. Whereas other kinds of consumers may not take action, privacy and data create powerful incentives for health app users to sue to enjoin a company from sharing their data and to recover damages for lost privacy. If courts use these opportunities to police abusive amendments, those decisions will have spillover effects. Favorable precedents in the digital health tech context could help consumers in other situations where suing for abusive unilateral amendments is cost prohibitive. And incremental

313 Burton, *supra* note 306, at 383–84.

314 *See, e.g.*, James v. Nat'l Fin., LLC, 132 A.3d 799, 814 (Del. Ch. 2016) ("This court has identified ten factors to guide the analysis of unconscionability.").

315 Bridgeman & Sandrik, *supra* note 186, at 397.

316 Bar-Gill & Davis, *supra* note 177, at 38.

reform is better than no reform at all. Even if the parties settle, reversing unfavorable changes in terms could be part of the settlement agreement, which could benefit all of the health app's users, not just the ones that sued. For reasons of efficiency alone, companies should want to have uniform terms across their customers, as monitoring and enforcing different agreements for different sets of users could be administratively burdensome.[317]

Lastly, arbitration clauses will not nullify the effect of courts in this area. In fact, arbitration clauses may not be as common as many people believe.[318] Of the health law apps we surveyed, less than a third included mandatory arbitration clauses in their ToS.[319] Even for those apps, parties may still have the ability to opt out of arbitration.[320] The fact that at least some companies do not force users to arbitrate means that courts will be able to affect not only judicial precedent but future arbitrations, should they adopt our recommendations.

Good faith also has potential doctrinal weaknesses. There is some dispute over whether the duty of good faith applies to unilateral amendments at all. Commentators have come to different conclusions, ranging from stating that a party unilaterally amending a

317 However, sometimes companies will act inefficiently to be able to share more data. *See* Ram & Roberts, *supra* note 113, at 707–08 (explaining that FamilyTreeDNA adopted different defaults for users depending on their jurisdiction).

318 This concern may be overblown not just in the context of digital health tech. Despite the general belief otherwise, arbitration agreements are not present in all ToS and privacy policies. For example, a decent number of credit card contracts do not have arbitration clauses. *See, e.g.*, Peter B. Rutledge & Christopher R. Drahozal, *Arbitration Clauses in Credit Card Agreements: An Empirical Study*, 9 J. EMPIRICAL LEGAL STUD. 536 (2012). Therefore, if any companies do not have arbitration clauses, courts will be able to affect arbitrations and subsequent judicial decisions through ruling like we suggest. Even if all contracts have arbitration clauses, a court could still be involved because it could say the unilateral amendment provision makes the entire contract illusory. If there is no contract, then the arbitration provision is ineffective, and the court would not compel arbitration.

319 Twenty-nine percent (8/28) included mandatory arbitration clauses: 40% of genetic apps (4/10), 20% of femtech apps (2/10), and 25% of mental health apps (2/8). Two apps included in this survey did not have terms of service (DTest and What's Up).

320 For example, one mental health app (Headspace) includes language that indicates a user may opt-out of the arbitration agreement contained in the ToS by default. To opt-out of the arbitration agreement, the user "must notify Headspace in writing no later than 30 days after first becoming subject to" the arbitration agreement. *See Terms & Conditions*, HEADSPACE, https://www.headspace.com/terms-and-conditions#arbitration [https://perma.cc/F3KE-WFXP] (May 18, 2021). The written notice must include specific information sent to either a physical address in California or an email address provided. *Id.* Notably, the app includes this information near the bottom of the terms of service, several paragraphs below the first mention of the arbitration notice. The initial Arbitration Notice and Class Action Waiver appears at section 1.2 in the Headspace Terms of Service. *Id.* Additional information about arbitration, including the ability to opt-out in writing, does not appear again until section 13.12. *Id.*

contract must act in good faith[321] to arguing that such a party has "unfettered power to alter deal terms in its favor."[322] The latter position, however, is ill-conceived. Every term of every contract has an implied obligation of good faith in the common law, the UCC, and the United Nations Convention on Contracts for the International Sale of Goods.[323] Indeed, "[t]he good-faith doctrine is probably one of the most fundamental principles in contemporary contract law."[324]

That said, good faith as currently applied might not seem like an effective tool against unfavorable one-sided changes. Some courts allow companies to engage in extremely abusive conduct despite the obligation of good faith because the companies are following the letter of the contract.[325] Scholars have thus concluded that good faith is a weak doctrine.[326] Nonetheless, courts could police truly egregious conduct, should they be inclined.[327] And indeed, courts are more likely to use good faith in consumer transactions than other types of cases,[328] making it a useful doctrine for courts and litigants to consider.

Overall, courts can protect health app users by imposing a robust duty to only modify contracts unilaterally in good faith. Giving consumers a viable cause of action for abusive unilateral amendments preserves the right of companies to make minor or reasonable modifications to update terms or to comply with new laws. At the same time, it offers a plausible claim for consumers to make when companies make unexpected or abusive amendments. While not the first-best solution, the doctrine of good faith could nevertheless be an important tool for protecting consumers while giving legislators and regulators the necessary time to act.

---

321 David Horton, *Indescendibility*, 102 CALIF. L. REV. 543, 568 (2014).

322 Andrea M. Matwyshyn, *Privacy, the Hacker Way*, 87 S. CAL. L. REV. 1, 61 n.273, 67 (2013).

323 United Nations Convention on Contracts for the International Sale of Goods art. 7(1), Apr. 11, 1980, S. Treaty Doc. No. 98-9 (1983), 1489 U.N.T.S. 3.

324 Alan D. Miller & Ronen Perry, *Good Faith Performance*, 98 IOWA L. REV. 689, 690 (2013).

325 *See, e.g.*, Kham & Nate's Shoes No. 2, Inc. v. First Bank of Whiting, 908 F.2d 1351, 1357 (7th Cir. 1990) ("Firms that have negotiated contracts are entitled to enforce them to the letter, even to the great discomfort of their trading partners, without being mulcted for lack of 'good faith.'").

326 Bar-Gill & Davis, *supra* note 177, at 17.

327 *See, e.g.*, In re 604 Columbus Ave. Realty Tr., 968 F.2d 1332, 1362 (1st Cir. 1992) (holding that the reasoning in *Kham & Nate's Shoes* did not prevent the court from considering a party's conduct inequitable).

328 James P. Nehf, *The Impact of Mandatory Arbitration on the Common Law Regulation of Standard Terms in Consumer Contracts*, 85 GEO. WASH. L. REV. 1692, 1705 (2017).

* * *

Consumers are in need of better protection against unfavorable unilateral amendments, both in digital health tech and beyond. Any intervention designed to regulate one-sided changes must be flexible enough to allow companies to modify their ToS and privacy policies in ways that could benefit their users. Here, we have outlined some potential strategies for striking that difficult balance. Legislative, regulatory, and judicial solutions all have their advantages and their drawbacks. A tiered approach that combines all three may in fact be the best way of protecting consumers. In the near-term, judges can act now using the doctrine of good faith to police predatory unilateral amendments. In the mid-term, the FTC—ideally with increased resources—could develop guidance and take enforcement actions. And in the longer term, Congress could enact comprehensive but flexible consumer protection legislation that not only gives Americans better control over their data but also requires companies to obtain consent before making material changes to their terms.

CONCLUSION

Unilateral amendment clauses allow companies to break their promises to customers without facing legal consequences. The troubling reality is that even the most informed users who have taken the time to read ToS and privacy policies still remain vulnerable. At present, consumers have very few legal tools at their disposal for challenging unfavorable one-sided changes. Usually, their only choices are to accept the undesirable new terms or to stop using the product altogether.

The informed minority hypothesis has come under fire recently in light of evidence that no one reads consumer contracts. Yet our analysis has revealed an instance where individuals may actually read—and choose products based on—terms. We selected health apps as a case study because their consumers are more likely to read and to rely on terms of service or privacy policies. If the informed minority hypothesis was going to work anywhere, it should work here.

But even with an informed minority of users willing to shop for terms, consumer contracts remain dysfunctional. Suboptimal decisionmaking, incomplete risk information, high switching costs, and a lack of notice mean that a viable market for privacy cannot exist when ToS and privacy policies include unilateral amendment provisions.

Certainly, the stakes are particularly high in digital health tech where users entrust some of the most intimate details of their lives to digital health tech companies and switching costs are especially steep.

That being said, savvy consumers have reason to be concerned about privacy and data security well beyond this particular industry. As a society, we are increasingly dependent on technology. It is nearly impossible to function in the modern world without interacting with the major tech companies like Apple, Google, Facebook, and Amazon.[329] Not coincidentally, all of these tech giants are notorious data harvesters and data brokers.

Because the problem extends beyond digital health tech, our solutions invoke contract and consumer law, not health law. We argue that companies should not be able to unilaterally amend terms in ways that are harmful to consumers. Ideally, federal legislation would require companies to consult with their customers before making material changes to their agreements. Current users who object to the change should have the opportunity to keep their original terms. Additionally, the FTC could take enforcement actions to protect consumer privacy, as well as educate users about their rights and offer guidance to companies about best practices. Finally, courts can adopt a more robust interpretation of the duty of good faith to ensure that companies are straightforward with consumers when they change terms. Congress, the FTC, and judges should work in concert to better protect consumers against unilateral amendment clauses, which currently render all terms uncertain.

329 *See* Kashmir Hill, *I Tried to Live Without the Tech Giants. It Was Impossible*, N.Y. TIMES (July 31, 2020), https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html [https://perma.cc/VFL3-SYLZ].

APPENDIX

In this Appendix, we provide the details of our study described in Part I. Our full dataset is available upon request.

A. Methodology

We identified the apps by searching the Apple App Store using a combination of the following terms: "DNA," "fertility," and "mental health." To replicate how a consumer might locate an app, we downloaded the first ten apps meeting the criteria based on the order they appeared in the App Store. We excluded genetic apps that did not allow a user to upload genetic information, even if only for the purposes of storing. We excluded one fertility app that only provided guided meditations. We excluded one mental health app that generated motivational quotes. In all three categories, we excluded apps requiring purchase to download or with ToS and privacy policies unavailable in English.

We selected a variety of apps handling sensitive health information. Those apps include "femtech" apps providing period and fertility tracking functions; mental health apps providing diagnostic or self-guided therapy services; and those storing, analyzing, or otherwise handling genetic information. We limited our analysis to thirty apps, with ten apps in each category.[330] We did not restrict our analysis to apps with corporate offices in the United States or those providing services that definitively fall outside the purview of the Food and Drug Administration's regulation of "devices." Instead, we focused on apps consumers are likely to encounter through a typical search in their smartphone-specific app stores.[331]

Unilateral amendment provisions are available in the ToS and privacy policies. These are generally available to users in the app, through an in-app link to the website, as a link from the App Store, or through a web search. In rare cases, a consumer must correspond with customer support to access ToS and privacy policies. For each app, an author (Fowler) downloaded the ToS and privacy policies.[332] All readily available policies were collected from company websites and apps and saved as electronic documents. Privacy policies were typically available as a link in the Apple App Store or at the bottom of the main

330 This sample size is not intended to be statistically significant or reflect the typical practices of *all* apps within a specific category of health app.

331 Where a user obtains apps will be specific to the type of device they own and their preferences. Common app stores include, but are not limited to, the Apple App Store, Google Play Store, or BlackBerry App World.

332 Given that ToS and privacy policies can and do change with regularity, PDF copies of the ToS and privacy policies used for this analysis are on file with the authors.

page on a company's website. In some instances, the ToS or privacy policies were only accessible through the app or direct correspondence with customer service representatives.

Our study sought to assess the prevalence of unilateral amendment provisions and the ways in which health apps communicate updates of terms and policies to users. To do so, we captured unilateral amendment language verbatim from ToS and privacy policies when present. Not all ToS and privacy policies contain specific headers labeling the text as a unilateral amendment clause. In addition to capturing language under such headers, we also conducted searches for words like "change," "modify," "alter," and "amend." If those terms were associated with additional language indicating unilateral modification, we captured the text as a unilateral amendment provision.

We then conducted a content analysis of unilateral amendment provisions.[333] We coded for language indicating if the app would notify the user and, when applicable, how the app intends to inform the users. We also coded for language explicitly stating that users must revisit ToS and privacy policies periodically to remain apprised of the contents. Additional considerations included statements about the date at which modifications would become effective, manner of acceptance of modified terms, and any information for users wishing to object to the modifications. In some cases, the unilateral amendment clearly stated that it would or would not act, for example, by always sending an email to a user in the event of a change. In those cases, we coded in the affirmative or negative, respectively. In other cases, the unilateral amendment was silent on what action would or would not be taken or indicated conditional language (e.g., "may" or "[w]e will notify you by email, through the App, or by presenting you with a new version of the Agreement for you to accept *if we make modifications that materially change your rights*"[334]). In those cases, we coded it as discretionary as it is unclear what the app will consider a material change of rights.[335]

---

333 Two research assistants (Taylor Hood and Jennifer Pier) independently coded the terms. An author (Leah R. Fowler) then reconciled the data and resolved inconsistencies.

334 Flo Terms of Use, January 2020 (emphasis added). Current terms of use available at https://flo.health/terms-of-service [https://perma.cc/67F4-QUB9].

335 We would like to offer a note on the potential subjectivity of our interpretations. ToS and privacy policies are notoriously difficult to read—even for highly motivated consumers. Analysis of reading levels often reveals that a user would need years of postsecondary education to understand these digital contracts fully. It is often joked that one would need to attend law school or be a lawyer to enter these contracts with eyes wide open. Our research assistants were third-year law students. According to analyses of Flesch-Kincaid readability, they should be able to understand these terms with relative ease. *See*

B. List of Apps Surveyed by Type

1. Femtech Apps

   Flo
   Glow
   Ovia
   Clue
   Fertility Friend
   Kindara
   Ovulation Calculator
   Natural Cycles
   OvuSense2
   Ava

2. Mental Health Apps

   Moodpath
   Daylio Journal
   Remente – Self Improvement
   Headspace
   Youper
   Depression Test
   Vent – Express Your Feelings
   What's Up – A Mental Health App
   Woebot – Your Self Care Expert
   Peak – Brain Training

3. Genetics Apps

   AncestryDNA
   23andMe
   MyHeritage
   Genomapp, Squeeze your DNA
   DNA2Tree
   Smart DNA MyGenomeBox
   Gini – DNA Based Nutrition
   DNA ID
   All of Us
   Genetica

Fowler, Gillard & Morain, *supra* note 241, at 68. However, throughout the data collection process, this proved to be a challenging undertaking.