THE FRAGILITY OF CONSENT

*Lori Andrews**

When I woke up one day last April, I was locked out of my iPhone. No, not by hackers, but by Apple itself. The message on the screen indicated that there were new terms of service and said, "If you do not agree to the terms of this license, you may return the iOS device . . . to the Apple Store . . . for a refund."

Of course, returning the phone was not an option. My photos for the past few years were on it, including the last pictures of my younger sister before she died. The device also housed my phone directory. The ones I could recite from memory were limited—those of my son, an ex-boyfriend, a college friend, and my office. For me, it was as if someone was holding my possessions hostage, asking me to give up basic human rights—like privacy—to get them back. I didn't want to agree to have my photos in the cloud. The proposed transaction did not fit my idea of consent. Where were all those new rights I supposedly had in wake of the GDPR?[1]

The process of consent in the app era has eroded considerably from its legal roots. It has come untethered from the idea of an informed and voluntary choice. Battered and debilitated, it no longer resembles the concept that I learned in a law school course titled "Informed Consent," that I wrote about in academic articles[2] and chapters,[3] or that I discussed in

* Lori Andrews, J.D., is the Director of the Institute for Science, Law and Technology and Distinguished Professor of Law at IIT Chicago-Kent College of Law. She received her B.A. from Yale College and her J.D. from Yale Law School.

1. The European Union's General Data Protection Act, https://eugdpr.org/the-regulation/, expanded the rights of digital service users in Europe and caused developers cross the globe to change the way they do business. Regulation (EU) 2016/679 of the European Parliament and 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 (General Data Protection Regulation), 2016 O.J. (L 119/1). *See also* Filippo A. Raso, Note, Innovating in Uncertainty: Effective Compliance and the GDPR, HARV. J.L. & TECH. DIG. (2018).

2. Lori Andrews, *Informed Consent Statutes and the Decision-making Process*, 5 JOURNAL OF LEGAL MEDICINE 163 (1984); Lori Andrews, *The Rationale Behind the*

consultations with federal agencies and professional organizations.

With her book, *Consentability: Consent and Its Limits*, Professor Nancy Kim provides a comprehensive analysis of the role of—and limits to—consent in modern society.[4] By applying her astute observations, we can find a way to counter the contemporary assaults on consent.

Professor Kim describes the trilogy of requirements for consent: "an intentional manifestation of consent, knowledge and action/voluntariness."[5] The legal principle of consent has the goal of protecting the consumer's dignity, privacy, and autonomy, as well as protecting the consumer from psychological, physical, and financial harms.[6]

Based on a study we undertook at the Institute for Science, Law and Technology (ISLAT) at IIT Chicago-Kent College of Law analyzing medical and psychiatric apps, I will discuss those requirements in the chronological order in which the consumer encounters those conditions. The first is knowledge—sufficient understandable information to provide the foundation for a true consent. The second is voluntariness. Voluntariness must be "intended rather than reflexive"[7] and must be free of "undue pressure or coercion."[8] The third is the manifestation of consent. This must be explicit, rather than implied. Just because I visit a surgeon's office, for example, does not mean that I consent to whatever surgery she is proposing. Nor should my use of an app mean that I consent to the collection of my private information for marketing purposes, to the activation of the microphone on my

---

Informed Consent Doctrine, 1 MEDICAL PRACTICE MANAGEMENT 59 (1985); Lori Andrews, *The Right and Rite of Informed Consent*, 21(5) LAW & SOCIETY REVIEW 765 (1988); E.W. Clayton, K.K. Steinberg, M.J. Khoury, E. Thomson, L. Andrews, M.J.E. Kahn, L.M. Kopelman & J.O. Weiss, *Informed Consent for Genetic Research on Stored Tissue Samples*, 274 JAMA 1786 (1995); and Lori Andrews, Kayla Kostelecky, Stephanie Spritz, & Alexandra Franco, *Virtual Clinical Trials: One Step Forward, Two Steps Back*, 19 JOURNAL OF HEALTH CARE L. AND POL'Y 189 (2017).

3. *See* chapters dealing with informed consent in LORI ANDREWS, MEDICAL GENETICS: A LEGAL FRONTIER (1987) and LORI ANDREWS, FUTURE PERFECT: CONFRONTING DECISIONS ABOUT GENETICS (2001).

4. NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019).

5. *Id. at 9.*

6. *See supra* note 1 and accompanying text.

7. KIM, *supra* note 4 at 9.

8. *Id.*

phone, or to the use of cookies or other tracking mechanisms to collect information about other things I do on my phone.

THE ISLAT STUDY

In the ISLAT study, we assessed hundreds of medical and psychiatric apps relating to diabetes, bipolar disorder, suicide prevention, and eating disorders.[9] The apps required users to enter sensitive information such as treatment regimes, AIDS status, suicidal thoughts, sexual practices, illegal drug use, and credit card numbers (for ease in refilling prescriptions through the app).

We analyzed the information the app developer provided to the consumer in advance of downloading the app so that the consumer could make an informed choice about whether to download and to use the app. We also studied the apps in action, assessing what information they were collecting from the user's phone and what they were transmitting from the phone. This allowed us to see if the apps were complying with what they promised in their privacy policies. Based on this study, we can discern whether the process for engaging with these apps met Nancy Kim's (and the law's) standard for consent.

KNOWLEDGE

The knowledge component of consent was undercut by virtually all the apps we studied because their privacy policies did not provide adequate information upon which to base a decision about whether to download or use the app. Privacy policies, where they exist, purport to describe how an app will interact with your phone (for example, whether it will use cookies or turn on the microphone), whether it will collect other information from your phone (such as your location, web searches, or contacts) and whether it will share or monetize your private information.

The absence, inaccessibility, incomprehensibility, and inaccuracy of privacy policies prevented users of apps from obtaining the information they needed to ensure a valid consent. Only 19% of medical apps and 38% of psychiatric apps even had privacy policies. The thousands (or perhaps even millions) of

9. For more information about the study, *see* Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421 (2018) and Sarah Blenner, Melanie Köllmer, Adam Rouse, Nadia Daneshvar, Curry Wiliams, & Lori Andrews, *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*, JAMA 1051 (2016).

people using these apps could not possibly have "consented" since they were not told what would happen to their information. In fact, the app users might be surprised or appalled to learn that the 79% of the medical apps with no privacy policies were sharing their information with unrelated third parties and that most of the apps were putting tracking mechanisms (such as cookies) on their phone.

Where they exist, privacy policies are often difficult to find. While many privacy policies are available on Google Play or the iOS App Store prior to download, others require the potential user to figure out the identity of the developer and track down the privacy policy on the developer's website. For example, in our study, for seven of the twenty-six bipolar apps that had privacy policies, those policies were only available on the developer's website. And sometimes it was unclear whether a privacy policy on the developer's website applied only to the website itself or to a specific app. Some of the privacy policies linked from Google Play's app description applied to other products and services offered by the developer and at times even explicitly excluded the medical app. Our study also found that the privacy policies were sometimes difficult to understand or even incomprehensible, preventing the user from obtaining sufficient knowledge for a valid consent. Some policies deliberately used terms that obfuscated what the app did with information. For example, by saying the app only shares information with "affiliates" and "third-party service providers," the developer may give the impression of only sharing data with a small group. However, "affiliates" and "third parties" can mean any entity that pays the app developer for the user's information. Thus, even consumers who go to the effort of searching for apps' privacy policies and reading them may not understand the actual implications of developers' data practices.

Other researchers similarly found that privacy policies are not readily understandable and may deliberately obfuscate what is being done with the user's information, providing a false comfort for users of apps who do not realize how limited the protections really are.[10] Even app developers themselves admit to

10. Out of the 40 social networking sites examined in the study, 65% of them were unclear about whether or not they collected user data from external sources. Joseph Bonneau & Sören Preibusch, *The Privacy Jungle: On the Market for Data Protection in Social Networks in* THE EIGHTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS 2009) (arguing that websites specifically make their privacy policies difficult to read so that users do not know what privacy is offered). Similarly,

difficulties in understanding their privacy policies,[11] but this should come as no surprise considering the average reading level of health app privacy policies is above the twelfth grade level[12] and privacy policies are often intentionally bewildering.[13] Thus, consumers generally do not receive adequate accessible information about what data the apps will collect and share about them.

Some developers provide inaccurate information in their privacy policies. We learned this by comparing what the app developers' privacy policies said their diabetes and bipolar apps did with what the apps actually did. Some said they would not share information with other entities, yet they did. Others said they would encrypt information, but they did not.

The novelty of app technology means that consumers do not know what to look for when reading privacy statements. A consumer might assume that health information from consumer apps is protected by the privacy rules adopted pursuant to HIPAA, the Health Insurance Portability and Accountability Act[14] (it isn't).[15] She might assume that the app would transmit her information encrypted, yet twenty-five percent of the bipolar apps we studied sent out information unencrypted. One bipolar app sent out the user's password unencrypted; therefore, any network snooper, such as another person using the wireless at Starbucks or a fellow passenger on Southwest Airlines,[16] would

---

a study of the privacy policies of 20 free and popular (more than one million downloads) Android health and fitness apps that collect personal information, such as location, found that the privacy policies discussed user data retention and sharing procedures in vague terms or not at all. Most also did not clearly say why they were collecting and storing this data, nor did they state with whom they were sharing it. *See* Mark Rowan & Josh Dehlinger, *A Privacy Policy Comparison of Health and Fitness Related Mobile Applications*, 37 PROCEDIA COMPUTER SCI. 348, 354 (2014).

11. *See* Rebecca Balebako & Lorrie Cranor, *Improving App Privacy: Nudging App Developers to Protect User Privacy*, 12 IEEE SECURITY & PRIVACY 55, 56 (2014).

12. *See* Mark Rowan & Josh Dehlinger, *A Privacy Policy Comparison of Health and Fitness Related Mobile Applications*, 37 PROCEDIA COMPUTER SCI. 348, 354 (2014).

13. Irene Pollach, *What's Wrong with Online Privacy Policies?*, 50 COMM. ACM 103, 107 (2007).

14. Health Insurance Portability and Accountability Act Privacy Rule, 45 C.F.R. § 160 *et seq*. (2013).

15. *See* Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421 (2018).

16. *See* Steven Petrow, *I Got Hacked Mid-Air while Writing an Apple-FBI Story*, USA TODAY (Feb. 24, 2016), https://www.usatoday.com/story/tech/columnist/2016/02/24/got-hacked-my-mac-while-writing-story/80844720.

be able to see the user's password. Considering that people often use the same password for multiple purposes, this is particularly problematic.

The consumer might assume that the existence of a privacy statement means that their private information would be protected. However, our study found that the fact that a medical app had a privacy policy did not mean the app actually protected privacy. In fact, apps with privacy policies were slightly more likely to disclose information to third parties than those without privacy policies.[17]

The deficiencies in the information provided by the apps' developers and the fact that most apps did not have privacy policies means that the majority of people who are using medical and psychiatric apps did not have sufficient knowledge to actually consent to what is being done with the information collected about them through the apps.

VOLUNTARINESS

Without adequate knowledge, it cannot be said that people are "voluntarily" using apps. In addition, with medical and psychiatric apps, there can be social pressures to use the apps. Seven percent of physicians prescribe apps[18] and people may be unwilling to go against their doctor's recommendation. Employers may also insist on the use of a health app for wellness purposes and insurers may charge extra for health insurance if the person does not use a health or fitness app.[19] Additionally, Medicaid offers an app[20] and the recipient might be worried about

17. The study found that 79% of diabetes apps with privacy policies disclosed information to third parties, compared to 76% of those without privacy policies. *See* Blenner et al., *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*, 315 J. AM. MED. ASS'N 1051, 1051 (2016).

18. Amy M. Bauer et al., *Use of Mobile Health (mHealth) Tools by Primary Care Patients in the WWAMI Region Practice and Research Network (WPRN)*, 27 J. AM. BOARD FAM. MED. 780, 784 (2014).

19. *See* Christopher Ingraham, *Should You Hand Over Your Fitbit Data to Your Insurer?*, HARTFORD COURANT (Sept. 27, 2018), https://www.courant.com/consumer/hc-ls-fitbit-health-data-20180930-story.html.

20. Medicaid provides medical apps to the people it covers in order to reduce health care costs by assuring greater compliance in taking medications and attending doctors' visits. *See UnitedHealthcare Launches Mobile App to Help Medicaid and CHIP Beneficiaries More Easily Navigate the Health System*, UNITEDHEALTH GROUP (Aug. 11, 2015), http://www.unitedhealthgroup.com/Newsroom/Articles/Feed/UnitedHealthcare/2015/0811MedicaidCHIPHealth4Me.aspx. While currently app use is currently "voluntary," Medicaid beneficiaries may be concerned

losing coverage if she does not use it.

MANIFESTATION OF CONSENT

The evidence that consent has manifested in the app realm is extremely weak. Should a developer be allowed to claim that a person has consented merely because she uses an app? Did I really consent to dictionary.com putting 234 cookies[21] on my computer when I looked up the spelling of a word (when I wasn't even told of that possibility)? What if I clicked a button saying, "I consent"? Or gave in when Apple ransomed my phone by threatening to cut off my access to it unless I agreed to their new policies?

Given the number of apps and online platforms that people consult on a daily basis and the length of disclosure forms, it is not humanly possible to read, process, and apply all the privacy policies with which a modern individual comes in contact. Most people just click "okay."[22] Even though the disclosure of information from apps can have financial, psychological, and physical impacts, there are far too many digital privacy policies for people to process, and those policies that do exist are hard to locate and hard to understand.[23] A Carnegie Mellon study found that it would take a person thirty days to read the privacy statements of the apps and websites that she commonly uses.[24]

Even if an app user makes the effort to read all relevant privacy policies, app developers make no commitment to continue to honor those policies. Despite captioning these statements as

---

about losing benefits if they don't download and use the app.

21. *Tracking the Companies That Track You Online*, FRESH AIR (Aug. 19, 2010), www.npr.org/templates/story/story.php?storyId=129298003; Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 31, 2010, at W1.

22. A 2013 survey of 584 university students between the ages of 18 to 53 found that 85% of respondents reported that they do not completely read a privacy policy for an app, website, or social network. *See* Mark Rowan & Josh Dehlinger, *Privacy Incongruity: An Analysis of a Survey of Mobile End-Users*, PROC. OF THE INT'L CONF. ON SECURITY AND MGM'T 24 (2014), http://worldcomp-proceedings.com/proc/proc2014/sam/SAM_Papers.pdf.

23. *See* Florian Schaub, *Nobody Reads Privacy Policies—Here's How to Fix That,* THE CONSERVATION (Oct. 9, 2017), http://theconversation.com/nobody-reads-privacy-policies-heres-how-to-fix-that-81932.

24. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A J. L. & POL'Y FOR INFO. SOC'Y 543, 562–63 (2008) (noting that it would take the average individual 244 hours per year to read all the online privacy policies they accept, equivalent to about ten 24-hour days of reading or roughly 30 eight-hour workdays of reading).

"privacy policies," some policies say they give rise to no rights,[25] while others say that they can change their terms at any time.[26] In other words, just because the developer has agreed to protect privacy before the user downloads the app does not mean that that provision will be honored as the user interacts with the app in the future. Why should I be held to have agreed to the terms of service that the app has put in place when the developer is not similarly bound?

UNILATERAL CHANGES IN PRIVACY POLICIES

The problems of consent are multiplied by the bait-and-switch tactics that app developers use. Let's say that you have diabetes or bipolar disorder and take the time to do research on the hundreds of relevant apps that are available for each condition. You find that a minority of them have privacy policies and you decide that you are going to limit your search to ones with a privacy policy, figuring that at least you will know what you are getting into if the app describes its policies in advance. You find one that fits your criteria. It will encrypt your information, it will not share your health or location information with third parties, and it will not put cookies on your phone or collect information from other apps and functions of your phone.

You download the app, use it, and then, one night, it scoops up all your sensitive information (such as your difficulty keeping your diabetes in check, your suicidal thoughts, and your location) and sells it to marketers and life insurers. How could that happen? It could happen because most of the apps we studied said they could change their policies at any time.

Think about how odd that concept is. How can I consent to something when I don't know what it is or will be? How can a contract be so unilateral? How can the very provisions that I agreed to or paid for be taken away without explicit notice? How can the privacy protections that I chose an app for be dismantled, potentially causing me psychological, physical, or financial harm?

---

25. *See* WHATSMYM3, *Privacy Policy*, https://www.whatsmym3.com/Home/PrivacyPolicy (last visited Mar. 2020) ("This Privacy Policy is not intended to and does not create any contractual or other legal rights on behalf of any party.").

26. Nineteen of the 26 bipolar disorder apps with privacy policies (73.08%) indicated in their privacy policies that the terms and conditions of their privacy policies can be changed at any time. For example, Consurgo noted that their "Privacy Policy may be updated from time to time for any reason." *See* CONSURGO APPS, *Privacy Policy* (Aug. 13, 2015), http://consurgoapps.tumblr.com/post/126580646346/privacy-policy.

But that is exactly what happens with many medical and psychiatric apps.

Seventy-three percent of the bipolar apps we studied said that the terms of their privacy policy could be changed at any time. None of them said that they would definitely email the person and give her the choice of whether to agree to the new terms. Unlike a health care professional who cannot abandon you without referring you to another practitioner, a medical or psychiatric app can dump you if you don't agree to its new terms without finding you another app that would continue to serve you in the way you initially requested.

There is almost nothing you can do to protect yourself against this horrible outcome. None of the privacy policies of the medical and psychiatric apps provide for the knowledge, voluntariness, or manifestation of consent that would be required to ensure that your consent (or refusal) is garnered before the changes are made. Instead, the procedure generally goes as follows: a new privacy policy is posted to the developer's website, different from the one to which you originally agreed. You are responsible for continuously monitoring the website to look for changes. (A few apps' privacy policies that we studied states that they would change the date when there is a new policy,[27] but none said they would highlight the changed portion.). This generally means that you have to read the privacy policy in its entirety and figure out how it has changed. Your continued use of the app is taken to mean that you have consented to the changes.

Various apps' privacy policies tell you how often you should be checking to see whether the privacy policy has changed. For the bipolar apps we studied, some said to check it periodically.[28] One stated that a user should check "regularly,"[29] another from "time to time,"[30] one "frequently,"[31] and one "occasionally."[32] For

27. AFTER SCHOOL, *Your Privacy*, https://afterschoolapp.com/privacy/ (last visited Mar. 2020).

28. EXCEL AT LIFE, *Privacy Policy*, https://www.excelatlife.com/privacy_policy.htm (last visited Mar. 2020); RXWIKI, *Privacy Policy*, http://www.rxwiki.com/site-policies/privacy-policy (last visited Mar. 2020); WHATSMYM3, *Privacy Policy*, https://www.whatsmym3.com/Home/PrivacyPolicy (last visited Mar. 2020).

29. *See* CONSURGO APPS, *Privacy Policy* (Aug. 13, 2015), http://consurgoapps.tumblr.com/post/126580646346/privacy-policy.

30. WAG MOBILE INC., *Terms of Use, Privacy and Security Policy*, https://www.golearningbus.com/tou/ (last visited Mar. 2020).

31. DRUGS.COM, *Mobile Application Privacy Policy*, http://www.drugs.com/support/privacy-apps.html (last visited Mar. 2020).

the eating disorder apps we studied, 58% said their privacy policies could be changed at any time. Different apps advised that the user check "periodically,"[33] "regularly,"[34] or "often"[35] for changes. Some apps say they will only provide information when, in their sole discretion, the change is material.[36] This goes against the autonomy rationale underlying the legal requirement of consent—that it is up to the consumer to decide what information is material when deciding whether to buy a product, undergo a medical intervention, or, in this case, continue to use an app.

The conditions for legally adequate consent are sorely lacking for the initial use of medical and psychiatric apps and are even more problematic when the developer changes the privacy policies. The private information you tried so hard to protect by choosing a particular app can be disclosed and sold the moment a new policy goes into effect and you won't even know until you next check the privacy policy. You not only have to keep checking the privacy policies of your diabetes and bipolar apps, you have to check the policies of all the other apps and services you use (particularly because some of them collect information from your health apps). That's another thirty days each time you have to inventory the privacy policies of the apps and digital services you commonly use. And you are advised to do that complete review "frequently" or "often." When will you sleep or work?

SOLVING THE PROBLEMS OF CONSENT IN THE CONTEXT OF MEDICAL APPS

The legal standard for consent is not being met in the apps context. Knowledge is insufficient, coercion has replaced voluntariness, and consent is not adequately manifested. The

32. MED HELPER, *Privacy Policy*, http://medhelperapp.com/privacypolicy/ (last visited Mar. 2020).

33. UNDER ARMOUR, *Privacy and Terms*, https://account.underarmour.com/privacy?locale=en_US; Recovery Record, "Privacy Policy," https://www.recoveryrecord.com/privacy_policy/; RXWIKI, *Privacy Policy*, http://www.rxwiki.com/site-policies/privacy-policy (last visited Mar. 2020).

34. *See* CONSURGO APPS, *Privacy Policy* (Aug. 13, 2015), http://consurgoapps.tumblr.com/post/126580646346/privacy-policy.

35. MMAPPS MOBILE, *Privacy Policy of Mmapps Mobile*, http://mmappsmobile.com/privacy-policy/ (last visited Mar. 2020).

36. For example, "MoodPanda – Mood Diary Tracker" stated, "If we make a change to this policy that, in our sole discretion, is material, we will post information on the website." MOODPANDA, *Privacy Policy*, https://moodpanda.com/privacy.aspx (last visited Mar. 2020).

sheer number (and lack of uniformity) of terms of service and policy policies that we encounter each day makes it impossible for a consumer to protect herself through the consent process. So, what can be done?

We need to adopt policies that provide adequate protection as we do in other situations where the conditions for consent are at risk. First, as I have argued elsewhere,[37] we should completely prohibit app developers from collecting and sharing certain types of personal information, such as health information. This is in keeping with Nancy Kim's analysis of whether a proposed activity should be consentable.[38] Second, we should require greater understandability and uniformity in privacy policies. One approach might be to create icons that indicate what happens to your information when you use an app. One icon might have multiple people on it to indicate your information is being shared with third parties, one might have dollar signs on it to indicate that your information is being commercialized in some way, another might have a magnifying glass on it to let you know that the app is looking at or collecting information from other apps or services or functions of your phone, another could have a map to indicate the app collects your geolocation, and another could have a computer code to indicate that it transmits some information without encryption. If the app does not do a certain thing, a line could strike through the icon. In this way, a user can more easily compare apps and pick an app that meets his or her needs.

Third, the app developer should be forbidden from changing any of the promises it has made to the consumer. If, for dire business reasons, it must renege on one of these promises, it should be required to find an alternative for the consumer that meets the consumer's criteria, just as a doctor who stops providing services to a patient must find another practitioner to whom to refer the patient.

Fourth, there should be severe penalties if the app developer behaves in a way that puts the consumer at risk or does something (such as share information with third parties or fail to encrypt information) that the developer did not disclose in advance or specifically promised not to do.

The legal requirements for consent are not being met in the

37. Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421 (2018).

38. NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 49 (2019).

world of apps. By helping us understand the whys and hows of consent, Nancy Kim's *Consentability* can help us solve that problem and many others.