A NEW PRIVACY PARADIGM IN THE AGE OF APPS

*Lori Andrews**

Tens of thousands of mobile medical apps are currently available; 58% of Americans use these apps to diagnose, monitor, manage, and even treat health problems and diseases. A wealth of sensitive information is fed into the apps directly by the user and is collected indirectly by the apps. In a unique empirical study, we analyzed the privacy policies and permissions of hundreds of mobile medical apps. Then we intercepted outgoing transmissions to track what happened to the information the apps collected. Our novel methodology allowed us to compare what apps' privacy policies say that the apps (and their developers) do with the users' information with what they actually do—and to assess whether current laws protected that information.

Over 70% of the medical apps we studied shared users' sensitive information with third party data aggregators, without the users' knowledge or consent. As a result, users' health data from medical apps was frequently marketed and sold to third parties including advertisers, insurers, and employers. Medical apps currently constitute a gaping hole in the privacy Americans have come to expect when it comes to their personal health information.

Mobile health apps are generally not covered by the federal Health Insurance Portability and Accountability Act ("HIPAA"), nor do common law privacy torts adequately cover their privacy breaches. A new privacy paradigm is necessary.

---

* Lori Andrews, J.D., is the Director of the Institute for Science, Law and Technology ("ISLAT") 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. The author would like to thank the many wonderful ISLAT researchers involved in this project: Kara Angeletti, Sarah Blenner, Nadia Daneshvar, Emily Edwards, Alexandra Franco, Michael Goodyear, Melanie Köllmer, Dan Sanders, and Curry Williams. The author is deeply indebted to her administrative assistant Raymond Fang. She also benefitted from comments from her colleagues, including Hal Krent, Ellen Mitchell, Christopher Schmidt, Alex Boni-Saenz, Michael Gentithes, Cody Jacobs, Joan Steinman, and George Annas. She is also grateful for the feedback from attendees of her presentations at the Oklahoma City University School of Law and the National Institutes of Health Addressing ELSI Issues in Unregulated Health Research Using Mobile Devices Meeting.

This Article sets forth a controversial proposal—a prohibition against medical apps sharing information with data aggregators, marketers, or other third parties except, at the users' explicit request, the users' health care providers. This approach will protect users' privacy and improve the medical quality of apps.

TABLE OF CONTENTS

I. INTRODUCTION 422
II. MEDICAL APPS, DATA AGGREGATORS, AND ADVANCE NOTICE TO USERS 428
A. *The Use of Medical Apps* 428
B. *How Common Are Privacy Policies and How Accessible Are They?* 434
C. *Did the Apps with Privacy Policies Actually Protect Privacy?* 438
D. *The Significance of Permissions* 439
E. *What Did the Apps Actually Do With Information?* 441
III. CREATING A FRAMEWORK FOR PROTECTION OF INFORMATION FROM MEDICAL APPS 443
A. *The Rationale for the Protection of Health Information* 443
B. *Existing Protections Under HIPAA and Their Possible Expansion* 444
C. *The Federal Trade Commission* 447
D. *Existing Protection Under State Tort Laws and Their Possible Expansion* 449
1. *Intrusion on Seclusion* 450
2. *Public Disclosure of Private Facts* 452
3. *False Light* 455
4. *Unjust Enrichment* 457
IV. ALTERNATIVES TO EXISTING LEGAL POLICIES 460
A. *The Notice Model* 462
B. *A Ban on Disclosure of Information from Medical Apps* 465
V. CONCLUSION 468

I. INTRODUCTION

In 2017, a small self-funded team won an unusual $2.6 million prize.[1] The goal of the contest was to design a real-life equivalent of a device used by Dr. McCoy in *Star Trek*—his "tricorder," an

1. The team consisted of a doctor, his brothers, and friends. Beth Mole, *Underdog Team Wins Millions in Competition to Make Real-Life Tricorder*, ARS TECHNICA (Apr. 14, 2017), https://arstechnica.com/science/2017/04/underdog-team-wins-millions-in-competition-to-make-real-life-tricorder/.

automated diagnostic instrument.[2] The winning prototype—DxtER—turns an iPad into a tool that can help a person determine if she is suffering from any of thirty-four medical conditions.[3] DxtER, which purportedly can diagnose diabetes, pneumonia, atrial fibrillation, stroke, hepatitis, and other disorders,[4] is the tip of the iceberg in terms of digital technologies that allow patients to take their health into their own hands. Tens of thousands of mobile medical apps are currently available,[5] allowing consumers to diagnose,[6] monitor,[7] manage,[8] treat,[9] and prevent[10] health problems and diseases.[11] In many instances, medical apps are designed to take the place of a doctor.[12]

---

2. *See id.*
3. *See id.*
4. *See id.*
5. As of July 2018, Google Play had 41,886 apps in the medical category and 95,711 apps in the health and fitness category. *See Android Statistics – Category Statistics Table*, APPBRAIN, http://www.appbrain.com/stats/android-market-app-categories (last visited Jul. 26, 2018). The iOS App Store had 47,846 apps in the medical category and 74,871 apps in the health and fitness category. *See Store Stats – Category Distribution,* 42 MATTERS, https://42matters.com/stats (last visited Jul. 26, 2018).
6. Examples of apps that claim to help diagnose a condition include "Bipolar Disorder" by Deep Powder Software, "Bipolar Uncovered" by My Mean Apps, and "Bipolar Disorder" by Droid Clinic.
7. "Instant Blood Pressure" by AuraLife is designed to measure and monitor physiological parameters. *See How to Use Instant Blood Pressure*, INSTANT BLOOD PRESSURE, https://www.instantbloodpressure.com/how-to-use (last visited Aug. 10, 2018).
8. "BlueStar" by WellDoc is an example of an app that claims to help manage a health condition (type 1 diabetes). *See* Laura Lovett, *WellDoc's BlueStar Now Available on Solera Health's Marketplace*, MOBI HEALTH NEWS (Jan. 17, 2018), https://www.mobihealthnews.com/content/welldocs-bluestar-now-available-solera-healths-marketplace.
9. "UltimEyes" by Carrot Neurotechnology is an app to improve sight. William Herkewitz, *This App Trains You to See Farther: Twenty-Twenty Vision? Big Deal. UltimEyes Could Train Your Brain to See in 20/7.5*, POPULAR MECHANICS (Feb. 18, 2014), https://www.popularmechanics.com/science/health/a12915/this-app-trains-you-to-see-farther-16506910.
10. An example of an app that claims to prevent health conditions is "Noom Health: Chronic Disease Prevention" by Noom, Inc.
11. *See* MURRAY AITKEN & JENNIFER LYLE, PATIENT ADOPTION OF MHEALTH: USE, EVIDENCE AND REMAINING BARRIERS TO MAINSTREAM ACCEPTANCE 1–23 (2015); Andreas Michaelides & Ed Pienkosz, *Reaching Beyond the Exam Room: How Technology-backed Lifestyle Intervention is Improving Health Outcomes for Diabetes and Hypertension Management*, NOOM (Mar. 7, 2017), https://www.noom.com/in-the-news/2017/03/reaching-beyond-exam-room-technology-backed-lifestyle-intervention-improving-health-outcomes-diabetes-hypertension-management.
12. For example, "MelApp" and "Mole Detective" both claimed to diagnose melanomas even in their earliest stages through analyzing a picture of the mole taken by the user. *See* Karra, *A Cancer Detecting App? FTC Says No There's Not an App for That*, FTC L. (Apr. 23, 2015), http://www.ftclaw.com/2015/04/ftc-vs-mole-detective-and-melapp.

A medical app can help the user identify and manage health problems.[13] But the private information that a user enters into medical apps is also collected, shared, or sold, often without the app user's knowledge or consent,[14] to third parties which will use this information in ways that might harm the individual psychologically,[15] physically,[16] or financially.[17] Data aggregators' actions can even

13. *See, e.g.*, Morwenna Kirwan et al., *Diabetes Self-Management Smartphone Application for Adults With Type 1 Diabetes: Randomized Controlled Trial*, 15 J. MED. INTERNET RES. 235, 235–40 (2013); Charlene C. Quinn, *Cluster-Randomized Trial of a Mobile Phone Personalized Behavioral Intervention for Blood Glucose Control*, 34 DIABETES CARE 1934, 1940–41 (2011); Charlene C. Quinn et al., *WellDoc Mobile Diabetes Management Randomized Controlled Trial: Change in Clinical and Behavioral Outcomes and Patient and Physician Satisfaction*, 10 DIABETES TECH. & THERAPEUTICS 160, 161 (2008).

14. *See* Jay Hancock, *Workplace Wellness Programs Put Employee Privacy at Risk*, CNN (Oct. 2, 2015), http://www.cnn.com/2015/09/28/health/workplace-wellness-privacy-risk-exclusive/index.html. Third parties can use the information to price insurance premiums or evaluate an individual's credit score. A panel at an FTC workshop in 2013 warned that premiums could be changed based on data from wearables and apps. *See* STEPHANIE GILLEY, FEDERAL TRADE COMMISSION: INTERNET OF THINGS WORKSHOP 169 (2013), http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf. That has since become reality. *See* Reed Abelson, *Employee Wellness Programs Use Carrots and, Increasingly, Sticks*, N.Y. TIMES (Jan. 24, 2016), https://www.nytimes.com/2016/01/25/business/employee-wellness-programs-use-carrots-and-increasingly-sticks.html?_r=0; Parmy Olson, *Wearable Tech Is Plugging Into Health Insurance*, FORBES (June 19, 2014), https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#46ac72b818bd.

15. *See* Michael McFarland, *Why We Care About Privacy*, MARKKULA CTR. FOR APPLIED ETHICS, https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/why-we-care-about-privacy/ (last visited Aug. 10, 2018) (explaining how the exposure of people's personal information can lead to psychological harm or debilitation); *see also* Charles Ornstein, *Small Violations of Medical Privacy Can Hurt Patients and Erode Trust*, NPR (Dec. 10, 2015), http://www.npr.org/sections/health-shots/2015/12/10/459091273/small-violations-of-medical-privacy-can-hurt-patients-and-corrode-trust (providing an example of how a breach of medical data can afflict psychological harm to the affected individuals).

16. *See* Tom Garrubba, *5 Ways Health Data Breaches Are Far Worse Than Financial Ones*, HEALTHCARE IT NEWS (Nov. 10, 2014), http://www.healthcareitnews.com/news/5-ways-health-data-breaches-are-far-worse-financial-ones (noting that medical data breaches may result in physical harm or even death); Kashmir Hill, *Public Tracking Map Likely Led Rapist to Victim*, FORBES (July 25, 2012), www.forbes.com/sites/kashmirhill/2012/07/25/online-tracker-led-rapist-to-his-victim/ (noting that satellite tracking information was used to locate a woman and rape her); *see also* Lori Andrews et al., *Virtual Clinical Trials: One Step Forward, Two Steps Back*, 19 J. HEALTH CARE L. & POL'Y 189, 237 (2017).

17. Financial risk can occur due to having to pay more for goods such as life insurance. *See* BEYOND THE HIPAA PRIVACY RULE 181 (Sharyl J. Nass et al., eds., 2009) (explaining that a medical information breach can lead to health insurance and employment discrimination, resulting in financial harm); *see also* Michael McFarland, *Ethical Implications of Data Aggregation*, SANTA CLARA UNIV.: MARKKULA CTR. FOR APPLIED ETHICS (June 1, 2012), https://www.scu.edu

affect personal relationships.[18] As Commissioner of the Federal Trade Commission ("FTC") Julie Brill noted, "[I]nformation about some of the most sensitive aspects of our lives is available for analysts to examine without our knowledge or consent."[19]

Even though federal and state laws provide robust protections for health information in traditional medical settings, those protections do not apply to user-generated data from medical apps.[20] The most ubiquitous protection of health information—the privacy rule adopted pursuant to the federal Health Insurance Portability and Accountability Act ("HIPAA")[21]—covers only health information in the hands of health care professionals and health care institutions, not information from mobile health apps used by consumers.[22] State tort doctrines regarding privacy also fall short.[23] Medical apps currently constitute a gaping hole in the privacy Americans have come to expect when it comes to their personal medical information.

At first blush, it might seem that the solution would be to extend HIPAA to protect medical privacy in the digital realm, and some states have taken that approach.[24] Yet broadening the reach of HIPAA is insufficient. Medical apps represent a paradigm shift for privacy protection that requires a different regulatory approach. Medical app information differs from traditional health information due to the scope of the information collected, the nature of that information, and the context in which it is collected.

The *scope* of health information collected by apps is astonishingly broad. Medical apps collect information about the user's thoughts, actions, moods, sex life, symptoms, and responses to interventions.[25]

/ethics/focus-areas/internet-ethics/resources/ethical-implications-of-data-aggregation (warning that aggregated data can be transferred to a wide variety of marketers and may cause some people to be denied health insurance).

18. In *Spokeo, Inc. v. Robins*, Robins complained that data aggregator Spokeo had put up incorrect information about him on its website, including an incorrect economic status and a statement that he was married while in fact he was single. Justice Sotomayor pointed out during oral argument that incorrect facts can result in real harm: for example, women would be less likely to date a married man. "I will tell you that I know plenty of single people who look at whether someone who's proposed to date is married or not." Transcript of Oral Argument at 13:09, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339).

19. JULIE BRILL, KEYNOTE ADDRESS AT THE 23RD COMPUTERS FREEDOM AND PRIVACY CONFERENCE: RECLAIM YOUR NAME 8 (2013), https://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf.

20. *See infra* Subparts III.B–III.D.

21. Health Insurance Portability and Accountability Act Privacy Rule, 45 C.F.R. § 160 (2018).

22. *Id.* §§ 160.103, 160.502.

23. *See infra* Subpart III.D.

24. *See infra* Subpart III.B (discussing California and Texas statutes).

25. *See, e.g.*, *DBSA Wellness Tracker: Depression and Bipolar Support Alliance*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=org.facingus.tracker (last visited Aug. 10, 2018).

Data aggregators take that digital information, often without the user's knowledge or consent, and combine it with other information about her, such as data about her online and in-store purchases, whether she has cable television, who she phones most frequently, and where she is according to constant GPS monitoring.[26] Far more than the few bits of health information found in a doctor's file, medical apps allow data aggregators to achieve 24/7 monitoring in order to create a digital doppelgänger of the person.

The *nature* of health information collected through mobile apps is also profoundly different from health information collected in traditional medical settings. Medical apps collect personal information about the user both actively and passively. A medical app may know a person is ill before she does. For example, some apps use the accelerometer in the phone to measure a person's gait and the microphone to monitor a person's speech patterns.[27] Apps can diagnose the flu,[28] a stroke,[29] or Huntington's disease,[30] before the person experiences the first symptoms. This predictive feature of apps creates new challenges for privacy. People could keep health information private in the past by not disclosing the information to anyone, including a physician.[31] Or the person could seek medical services under a pseudonym, as was allowed in AIDS testing.[32] But gait and speech information can be collected by an app without the user's knowledge or consent. This information then can be surreptitiously shared with data aggregators and sold to third parties.[33] Thus, information about a user's health status that the user might not even know about herself can be disseminated with no

---

26. *See* BRILL, *supra* note 19.

27. Sue Hughes, *Slow Walking Speed May Signal Alzheimer's Risk*, MEDSCAPE (Dec. 3, 2015), http://www.medscape.com/viewarticle/855360.

28. ANMOL MADAN ET AL., SENSING THE 'HEALTH STATE' OF OUR SOCIETY 1–3 (2011), https://www.media.mit.edu/publications/sensing-the-health-state-of-our-society.

29. *See Smartphone App Can Detect Early Signs of Stroke*, UNIV. OF TURKU (Sept. 2, 2016), http://www.utu.fi/en/news/news/Pages/Smartphone-App-Can-Detect-Early-Signs-of-Stroke.aspx (university press release for app developed by its researchers that can detect atrial fibrillations through use of the phone's accelerometer and gyroscope).

30. *See* Mary Danoudis & Robert Iansek, *Gait in Huntington's Disease and the Stride Length-Cadence Relationship*, 14 BMC NEUROLOGY 161, 161–62 (2014).

31. For example, some people who feared discrimination based on genetic information chose not to seek medical information about their risk of genetic disease. *See* LORI ANDREWS, FUTURE PERFECT: CONFRONTING DECISIONS ABOUT GENETICS 130–50 (2001).

32. *See* The Ryan White HIV/AIDS Program, *Confidentiality: A Living History*, https://hab.hrsa.gov/livinghistory/issues/Confidentiality.pdf (last visited Aug. 10, 2018) (discussing the negative stigma connected to HIV as a deterrent for testing, which anonymous testing addressed).

33. *See* ROBERT J. ELLIS ET AL., A VALIDATED SMARTPHONE-BASED ASSESSMENT OF GAIT AND GAIT VARIABILITY IN PARKINSON'S DISEASE 10 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4627774/.

way for her to control the flow of that information. In some instances, information predictive of health status might not even be considered health information under any current legal definition. In one instance, Target sent pregnancy-related coupons to a teenage girl's home based on data analytics showing that an early sign of pregnancy is that a woman purchases unscented lotion, mineral supplements, and cotton balls.[34] The girl's father angrily criticized Target employees for assuming his daughter was pregnant, only to later apologize when he learned that the prediction was accurate.[35]

The *context* of medical apps' information collection practices is unique as well. When sensitive information is collected in a physician's office, the confidentiality of the information is not just protected by HIPAA. The entire context and policy environment of the physician-patient relationship safeguards that information. The Hippocratic Oath[36] and other medical ethics codes[37] protect physician-patient confidentiality. Doctors are required to protect the confidentiality of patient information under the common law doctrines of privacy, fiduciary duty, contract, negligence, and warranty.[38] Indeed, for the physician, "[t]he promise of secrecy is as much an express warranty as the advertisement of a commercial entrepreneur."[39] In contrast, medical app developers owe none of these duties to their users. Even if HIPAA were extended to cover medical apps, HIPAA provides no private cause of action and is itself insufficient in a context where no additional pressures (such as loss of medical license or fear of a tort action) create an incentive for the app developer to protect privacy.

This Article offers a unique perspective on the paradigm shift in health privacy by presenting data from empirical studies on the privacy policies of medical apps, their permissions, and their surreptitious transmissions. The studies, which were undertaken by the author and her colleagues at the Institute for Science, Law and Technology ("ISLAT") at Chicago-Kent College of Law, analyzed hundreds of medical apps related to diabetes, bipolar disorder, eating

34. Jordan Ellenberg, *What's Even Creepier Than Target Guessing That You're Pregnant?*, SLATE (June 9, 2014), http://www.slate.com/blogs/how_not_to_be_wrong/2014/06/09/big_data_what_s_even_creepier_than_target_guessing_that_you_re_pregnant.html.

35. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp.

36. *Hippocratic Oath*, NAT'L INST. OF HEALTH (Feb. 7, 2012), https://www.nlm.nih.gov/hmd/greek/greek_oath.html.

37. *See, e.g.*, *AMA Code of Medical Ethics: AMA Principles of Medical Ethics*, AM. MED. ASS'N (June 2001), https://www.ama-assn.org/sites/default/files/media-browser/principles-of-medical-ethics.pdf.

38. *See* LORI ANDREWS, MEDICAL GENETICS: A LEGAL FRONTIER 192–94 (1987); *see also infra* Subpart III.B.

39. *See* Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793, 801 (N.D. Ohio 1965).

disorders, and suicide.[40] We assessed the function of the apps and the types of information they collected. We determined what proportion of the apps had privacy policies and how the policies handled information collection, information dissemination, encryption, user choices, and future changes to the privacy policies. We analyzed the permissions of the apps—that is, the disclosures app developers made about how the app functioned and what aspects of the device an app accessed (such as GPS location, the phone's microphone or camera, the list of contacts, and so forth).

Our novel study allowed us to compare what apps' privacy policies say that the apps (and their developers) do with the user's information with what they actually do. We learned that sensitive information from medical apps is routinely disseminated in ways that harm app users, and that current laws do not adequately protect app users.

Part II of this Article discusses the extent to which medical apps are used, the type of information they collect, and how data aggregators access and disseminate that information. It then analyzes the types of notice privacy policies and permissions provide in advance about the medical apps' information collection and dissemination practices and assesses the transmissions to and from apps to determine how the actual practices compared to the advance notices. Part III discusses current gaps in legal protections for information collected by medical apps by analyzing HIPAA, FTC actions, federal statutes, state statutes, and the common law doctrines of intrusion on seclusion, public disclosure of private facts, false light, and unjust enrichment. Part IV proposes a framework for a new regulatory approach.

II. MEDICAL APPS, DATA AGGREGATORS, AND ADVANCE NOTICE TO USERS

A. The Use of Medical Apps

A significant number of Americans depend on medical apps as part of their medical care; 58% of smartphone users have downloaded a health app.[41] The choices are astonishing. As of July 2018, Google Play had 41,886 apps in the medical category[42] and 95,711 apps in the health and fitness category.[43] The iOS App Store had 47,846 apps

40. For an explanation of the methodology, see *infra* Subpart II.A.

41. Paul Krebs & Dustin T. Duncan, *Health App Use Among US Mobile Phone Owners: A National Survey* 3 JMIR MHEALTH AND UHEALTH 1, 5 (2015), http://mhealth.jmir.org/2015/4/e101/.

42. *Android Statistics – Category Statistics Table*, *supra* note 5.

43. *See id.*

in the medical category[44] and 74,871 apps in the health and fitness category.[45]

Apps have also made their way into the traditional health care system. Approximately 7% of primary care physicians have recommended a health app to a patient.[46] Physicians who prescribed apps recommended on average 1.74 apps per patient per visit.[47]

In addition, medical apps and wearables like Fitbit[48] that monitor an employee's activities and health are becoming increasingly common in the workplace.[49] Employees are sometimes pressured into participating in a workplace wellness program; for example, Houston city employees were required to pay an extra three hundred dollars a year for medical coverage if they declined to participate in the workplace wellness program.[50] The company Houston hired to collect health data from the program had the power to share the data with third-party vendors and even post the data in areas "that are reviewable to the public."[51]

---

44. *Store Stats – Category Distribution*, *supra* note 5.

45. *See id.*

46. 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).

47. AITKEN & LYLE, *supra* note 11, at 20. IMS Health's AppScript product allows healthcare professionals to prescribe mHealth applications. This report reviewed the data from AppScript and determined that healthcare professionals using AppScript on average prescribed 1.74 apps per patient per visit. *Id.*

48. Lee Bell & Chris Hall, *Fitbit Ionic Review: Bridging the Gap Between Fitness Tracker and Smartwatch*, POCKET-LINT (June 21, 2018), https://www.pocket-lint.com/fitness-trackers/reviews/fitbit/142566-fitbit-ionic-review-fitness-tracker-smartwatch.

49. For example, GetHealth and CoreHealth offer apps designed for workplace wellness programs. *See* Allegra Thomas, *5 Tools for Tracking & Motivating Employee Wellness*, 2020 (July 14, 2017), https://www.2020onsite.com/blog/5-tools-for-tracking-motivating-employee-wellness. *See generally* Gordon Hull & Frank Pasquale, *Toward a Critical Theory of Corporate Wellness*, 13 BIOSOCIETIES 190 (2017); Kelli B. Grant, *Your New Office Workout: Financial Fitness*, CNBC (Apr. 23, 2016), http://www.cnbc.com/2016/04/23/workplace-financial-wellness-programs-get-more-popular.html.

50. Houston city employees, including the Houston Police Officers' Union, objected so strongly to Audax's policies that the city switched to a different health data collector. *See* Hancock, *supra* note 14. As of September 2017, the city of Houston still had an employee wellness program that requires non-participating employees to pay an extra three hundred dollars per year for medical coverage. *See Wellness Campaign FAQ's*, THE CITY OF HOUSTON, http://www.houstontx.gov/hr/benefits/wellness_campaign_faqs.html (last visited Aug. 10, 2018); *2018-2019 Wellness Program: Win for Life*, CITY OF HOUSTON, http://www.houstontx.gov/hr/benefits/wellness_campaign.html (last visited Aug. 10, 2018).

51. Hancock, *supra* note 14. Even if the employer claims it is receiving and sharing only aggregated data, medical app and Fitbit data is so rich in detail that individuals can be identified. Ira Hunt, the former chief information officer of the CIA, said that "you can be 100 percent identified, as an individual, by your Fitbit data. Why? Because no two persons' gaits or ways of moving are the same.

Further, the information from medical apps can be collected, disclosed, and sold to the user's disadvantage in various ways. The app developer (or data aggregator that contracts with the developer) can collect and market the information.[52] Or an unrelated data aggregator can collect the information via tracking mechanisms (such as cookies, web beacons, and bots) from other mobile apps, websites the person visits, or the phone itself.[53] The entity with access to medical app data can use it to market products and services to the individual,[54] entice the individual to participate in a medical study,[55] or make a social, moral, or medical judgement about the eligibility of a person for a benefit such as insurance[56] or a job.[57] In more nefarious

---

We can almost always figure out who you are based on that kind of incredibly rich detail." GILLEY, *supra* note 14, at 170–71.

52. *See infra* Subpart II.C.

53. *Id.*

54. For example, Google made $95 billion in 2017 from advertising, which was 86.9% of Google's total revenue that year. *Advertising Revenue of Google From 2001 to 2017 (in Billion U.S. Dollars)*, STATISTA, https://www.statista.com/statistics/266249/advertising-revenue-of-google/ (last visited Aug. 10, 2018); *Distribution of Google's Revenues from 2001 to 2017, By Source*, STATISTA, https://www.statista.com/statistics/266471/distribution-of-googles-revenues-by-source/ (last visited Aug. 10, 2018). Facebook made $39.9 billion from advertising in 2017, which was 98% of Facebook's total revenue that year. *Facebook's Annual Revenue From 2009 to 2017, By Segment (In Millions U.S. Dollars)*, STATISTA, https://www.statista.com/statistics/267031/facebooks-annual-revenue-by-segment/ (last visited Aug. 10, 2018). Sometimes this marketing can be detrimental to the wellbeing of the individual. In our bipolar app study, an ISLAT researcher entered a lethal dose of lithium (6000 mg.) into the four apps that asked the user to input the dosage of their medication. One of these apps brought up an advertisement claiming that it could get him discounted prices on lithium. *See Pill Reminder and Medication Tracker by Medisafe*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.medisafe.android.client (last visited Aug. 10, 2018).

55. Andrews et al., *supra* note 16, at 190–91.

56. A person's digital profile is increasingly used to determine eligibility for life insurance. Leslie Scism & Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, WALL ST. J. (Nov. 18, 2010), http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html.

57. An individual's medical app data could be used to figure out practically anything an employer would want to know about a potential employee, including whether the applicant will have higher-than-average medical costs. *See* Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you; Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html (noting that tracking technologies such as cookies and web beacons allow companies access to an individual's browsing patterns and gives them the ability to make assumptions about such factors as the individual's socio-economic status and medical conditions).. FTC Commissioner Julie Brill said that she was worried that data could be used to deny someone employment. *See* Joseph Walker, *Data Mining to Recruit Sick People*, WALL ST. J. (Dec. 17, 2013), http://www.wsj.com/articles/SB10001424052702303722104579240140554518458.

hands, information from medical apps can be harvested by hackers for purposes of identity theft or sale. In fact, on the black market, a person's medical information sells for fifty times what credit card information sells for.[58]

The wide array of information collected from medical apps can be used by data aggregators and their corporate clients to discriminate against individuals. For example, a consulting group advises life insurers to deny insurance or charge more if the person eats fast food, commutes to work, is an avid reader, or has friends who are skydivers.[59] Information about all those behaviors can be gleaned from medical apps. Fast food consumption can be tracked through health apps that collect information about a person's meals[60] or by the app's use of GPS to collect information about the user's location.[61] The app's use of an accelerometer can indicate how much the person drives.[62] The app's use of tracking mechanisms that collect information from web searches or from other apps (such as Amazon or Kindle) can indicate how much the person reads.[63] Medical apps that link to the user's social media pages can learn who has friends who are skydivers.[64]

Our empirical study provided a unique glimpse into the information collection and dissemination practices of medical apps.[65] Initially, we focused on apps related to a specific disease—diabetes, a

58. *See* Consumer Reports, *Hackers Can Profit Greatly by Stealing Your Health Data. Are You Protected?*, WASH. POST (Nov. 9, 2015), https://www.washingtonpost.com/national/health-science/hackers-can-profit-greatly-by-stealing-your-health-data-are-you-protected/2015/11/09/e1f126f6-5181-11e5-933e-7d06c647a395_story.html?utm_term=.ccf13bc3b1c3.

59. MIKE BETTY ET AL., PREDICTIVE MODELING FOR LIFE INSURANCE 10–14 (2010), https://www.soa.org/files/pdf/research-pred-mod-life-batty.pdf; Michael Fitzgerald, *Underwriting Using Social Networking Tools*, CELENT (Apr. 14, 2010), https://www.celent.com/insights/947788169.

60. *See* Beth Skwarecki, *Diet Tracker Showdown: MyFitnessPal v. Lose It*, LIFEHACKER (Feb. 26, 2017), https://lifehacker.com/diet-tracker-showdown-myfitnesspal-vs-lose-it-1792754350.

61. "AADE Diabetes Goal Tracker" by AADE is an example of an app that has access to the user's geolocation.

62. *See* Kit Eaton, *Driving App Lets You Know if You're a Demon or a Granny on the Road*, FAST CO. (May 2, 2011), https://www.fastcompany.com/1751090/driving-app-lets-you-know-if-youre-demon-or-granny-road.

63. In addition, the reading app collects information. *See* Steve Bell, *Hey, Did You Know Your Kindle is Spying on You? And Here's How to Stop It*, BULLGUARD (July 29, 2015), https://www.bullguard.com/blog/2015/07/did-you-know-that-your-kindle-is-spying-on-you-here-is-how-to-stop-it.

64. *See* BETTY ET AL., *supra* note 59.

65. In lieu of lengthy footnotes listing app names and the number of apps that we are reporting on throughout the paper, we have provided spreadsheets at https://drive.google.com/drive/folders/1T-nHthYf3Ha75hHumdmAh6tLcsOWZ1bx.

chronic disease that affects roughly one in eleven Americans.[66] A person with diabetes must manage her own condition, making diabetes well-suited for mobile health app-based management. In order to locate relevant apps, we searched the computer-based version of the Google Play Store using the search term "diabetes."[67] We downloaded all 211 diabetes apps from the Google Play Store, categorized the functions of the apps, assessed the available privacy policies, and analyzed the apps' permissions. We also tracked the transmissions of a subset of 65 of these 211 apps, 24 with privacy policies and 41 without. We intercepted all outgoing and incoming transmissions, decrypted lightly encrypted transmissions, and determined which functions the app ran on the device. We used a similar methodology with our study of 128 psychiatric apps. The psychiatric app study included three components: bipolar disorder apps, eating disorder apps, and suicide prevention apps.[68] We also

66. *See* CTR. FOR DISEASE CONTROL & PREVENTION, NATIONAL DIABETES STATISTICS REPORT, 2017 5 (2017) https://www.cdc.gov/diabetes/pdfs/data/statistics/national-diabetes-statistics-report.pdf.

67. The study identified 271 diabetes-related apps. Apps were omitted from our analysis if the app was removed from the Google Play Store during the six-month period following our initial search or if the app was not in English.

68. ISLAT researchers searched for the psychiatric disorder apps on Google Play using the terms "manic depression," "anorexia," "bulimia," and "suicide." Unlike with the diabetes apps, we discovered that many of the apps that purported to be about these psychological conditions did not actually deal with them. For example, we found 247 bipolar apps, but 162 were excluded from the study because they were either directed towards health care professionals or did not actually address bipolar disorder. A further 22 apps were removed because they were created by developers outside of the United States, leaving only 63 apps.

For the eating disorder apps, ISLAT researchers used the terms "anorexia" and "bulimia." The search for "anorexia" returned 122 apps and the "bulimia" search returned 63 apps. The majority of results overlapped between the two studies; those overlapping apps were only counted once. In addition, 47 apps were excluded due to being mainly for exercise purposes rather than specifically geared toward eating disorders, weight loss, or dieting, were designed for parents or health care providers, or were unrelated to eating disorders or weight loss. This left 82 apps. A further 49 were removed because they were created by developers outside of the United States. Only 33 apps were left in the end.

ISLAT researchers searched for suicide prevention apps on Google Play using the term "suicide." This search returned 248 apps, but 191 were excluded from the study because they were either directed towards health care professionals or someone who knew somebody suffering from suicidal thoughts or did not actually address suicide. This left 57 suicide prevention apps. A further 25 apps were removed because they were created by developers outside of the United States. Only 32 apps were then left for the analysis.

tracked the transmissions of a subset of 26 bipolar apps, all of those from our larger sample which had privacy policies.

These medical apps collected an extraordinary amount of information.[69] This information included such things as the user's self-reported mood,[70] sleep schedule,[71] medication information,[72] and personal health information including blood pressure,[73] cholesterol level,[74] menstrual cycle,[75] blood oxygen level,[76] and HIV status.[77] Other information included journaled personal thoughts, personal photos, doctors' appointments, illegal drug use, and how much time was spent with pets.[78] Some medical apps collected credit card information (to enable in-app ordering of medications)[79] or offered clinical services such as counseling.[80]

	All Apps Found on Google Play	**Apps Remaining After Removal of Ones Not Fitting the Category**	**Final Apps Remaining After Removing Foreign Apps**
Bipolar Apps	247	85	63
Eating Disorder Apps	185	82	33
Suicide Prevention Apps	248	57	32

69. According to the privacy policies we studied, 51% of diabetes apps and 82% of bipolar apps collected personal information. *See* spreadsheets at https://drive.google.com/drive/folders/1T-nHthYf3Ha75hHumdmAh6tLcsOWZ1bx.

70. *DBSA Wellness Tracker: Depression and Bipolar Support Alliance*, *supra* note 25.

71. *Id.*

72. *Id.*

73. *Id.*

74. *Id.*

75. *Id.*

76. *See, e.g.*, *Carezone*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.carezone.caredroid.careapp.medications (last visited Aug. 10, 2018).

77. *See id.*

78. *See id.*

79. If one opts into Carezone's Pharmacy Assistance CareZone Service, she can order medications from a pharmacy with a prescription. In this case, CareZone will collect the user's credit card information to pass along to the pharmacy to process payment for the medication. *See Privacy Policy*, CAREZONE (Sept. 11, 2017), https://carezone.com/privacy.

80. For example, the app Ginger.io is designed to connect users with what they call a "health coach," in order to help them talk through any mental health issues they might have. *See Ginger.io Emotional Support*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.ginger (last visited Aug. 10, 2018).

B. How Common Are Privacy Policies and How Accessible Are They?

Given the sensitivity of the information collected by apps, consumers might try to protect their health privacy by reading apps' privacy policies in advance and choosing an app that appears to protect privacy. There are several problems with that approach. Many—indeed most—medical apps do not have privacy policies.[81] Even when they exist, privacy policies can be difficult to locate and hard to understand.[82]

At ISLAT, we studied the privacy policies of diabetes apps, bipolar disorder apps, eating disorder apps, and suicide prevention apps. In each instance, only a minority of apps even had privacy policies that applied to the app.[83] Of the diabetes apps, only 19% had privacy policies. Of the psychiatric apps, only 38% had privacy policies.

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.[84] For example, 7 of the 26 bipolar app privacy 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 the developer's apps (and if the latter, which apps created by the developer).[85] Some of the privacy policies linked from Google Play's

---

81. In ISLAT studies on various mobile health apps, fewer than 50% had privacy policies. For diabetes, 19% had privacy policies. For bipolar disorder, 41% had privacy policies. For eating disorders, 36% and for suicide, 34%. *See also* LINDA ACKERMAN, MOBILE HEALTH AND FITNESS APPLICATIONS AND INFORMATION PRIVACY: REPORT TO CALIFORNIA CONSUMER PROTECTION FOUNDATION 22 (2013), https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf.

82. For example, 7 of the 26 bipolar app privacy policies in the ISLAT psychiatric app study were only on the developers' websites.

83. *See infra* Table 1. Our findings are in keeping with other studies of medical apps. *See* Kit Huckvale et al., *The Evolution of Mobile Apps for Asthma: An Updated Systematic Assessment of Content and Tools*, 13 BMC MED. 58, 58–60 (2015) (finding that 9% (7 of 78) of asthma apps released in or before 2011 had privacy policies, and 36% (33 of 92) of asthma apps released in 2012 and 2013 had privacy policies); KONSTANTIN KNORR ET AL., *On the Privacy, Security and Safety of Blood Pressure and Diabetes Apps*, *in* ICT SYSTEMS SECURITY AND PRIVACY PROTECTION 571, 576 (2015) (finding 19%, 29 of 154). Only one study of health apps found that more than half had privacy policies. *See* ACKERMAN, *supra* note 81 (finding 67%, 29 of 43).

84. *See infra* Table 1.

85. For example, in the bipolar app study, two apps' privacy policies were unclear about whether they applied to the app or the website. "T2 Mood Tracker" originally only mentions the website, but in the second line item it switches to refer to "this service." It is unclear if that means just the website or all services by the National Center for Telehealth and Technology, including the app. *See Security and Privacy Notice*, DEF. HEALTH AGENCY, http://t2health.dcoe.mil

app description pertained to other products and services offered by the developer and at times even explicitly excluded the app.[86]

Our study also found that the privacy policies were sometimes difficult to understand. Some policies deliberately used terms that obfuscated what the app did with information; for example, by saying the app only shares information with "affiliates"[87] and "third-party service providers,"[88] 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 if consumers put forth the effort to search for apps' privacy policies and read them, they may encounter conflicting information and not understand the true, long-term implications of developers' data practices. [89]

/privacy-policy.html (last visited Aug. 10, 2018). PSTEC's privacy policy refers only to "the PSTEC copyright holder and owner of this website." It is unclear if the copyright holder refers to the app itself. *See Terms of Use, Legal and Disclaimer*, PSTEC, http://www.pstec.org/legal.php#privacy (last visited Aug. 10, 2018).

86. For example, the eating disorder apps "Before I Eat," "Journal of Eating Disorders," and "RxWiki" had privacy policies that applied to the developer's website, but not the app itself. *See Privacy Policy*, STANDISH MEDIA, LLC (Sept. 6, 2017), http://standishmedia.com/privacy-policy; *Privacy Policy*, SPRINGER (May 1, 2018) http://www.springer.com/gp/privacy-statement/627414; *Privacy Policy*, RXWIKI (July 19, 2016), http://www.rxwiki.com/site-policies/privacy-policy/.

87.

> As used in this policy, the terms "using" and "processing" information include using cookies on a computer, subjecting the information to statistical or other analysis and using or handling information in any way, including, but not limited to collecting, storing, evaluating, modifying, deleting, using, combining, disclosing and transferring information within our organization or among our affiliates within the United States or internationally.

Privacy Policy, CAREZONE (Sept. 11, 2017), https://carezone.com/privacy.

88.

> If you choose to participate in any community-oriented parts of the Drugs.com App or web site, such as a forum, bulletin board, chatroom, Q&A, reviews or comments section, You should be aware that any personally identifiable information You choose to submit can be read, collected, used by others and may appear in search engines. Such information may also be shared with Our third-party service providers.

Mobile Application Privacy Policy, Drugs.com (May 22, 2018), http://www.drugs.com/support/privacy-apps.html.

89. *See generally* Adrienne Porter Felt et al., *Android Permissions: User Attention, Comprehension, and Behavior*, *in* PROCEEDINGS OF THE 8TH SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2012); Patrick Gage Kelley et al., *Privacy as Part of the App-Decision Making Process*, *in* PROCEEDINGS OF THE 31ST ACM CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 3393 (2013); Patrick Gage Kelley et al., *A Conundrum of Permissions: Installing Applications on an Android Smartphone*, *in* PROCEEDINGS OF THE 16TH FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 68 (2012).

Moreover, some of the privacy policies we analyzed in the ISLAT studies actively disavowed that they would protect privacy[90] or stated that they could stop protecting privacy at any time.[91] Of the 73% of bipolar apps whose privacy policies said that the terms and conditions could be changed at any time, 47% stated that continued use of the app after the changes means that the user accepts any changes to the privacy policy.[92] The privacy policy of one of the bipolar apps said that it provided no legal protections.[93]

Our results were consistent with other studies that similarly found that only a minority of health apps had privacy policies[94] and that in many cases it was difficult to locate and determine the applicability of privacy policies.[95] For example, one study of the 600 most commonly used iOS and Android health apps found that only 30.5% had a privacy policy; moreover, 66.1% of those did not address

90. "This Privacy Policy is not intended to and does not create any contractual or other legal rights on behalf of any party." *Privacy Policy*, WHAT'S MY M3, https://www.whatsmym3.com/PrivacyPolicy.aspx (last visited Aug. 10, 2018).

91. For example, the privacy policy of "Pacifica – Stress & Anxiety" stated that "any material changes will become effective 30 days from their posting on http://thinkpacifica.com/privacy.html or via email to your listed email address." The privacy policy could be changed at any time and would become effective, no matter the nature of its changes, shortly thereafter. *Privacy Policy*, PACIFICA (May 20, 2018), https://www.thinkpacifica.com/privacy.html.

92. For example, "Your ongoing use of 7 Cups indicates that you accept any changes to the Privacy Policy." *7 Cups Privacy Policy*, 7 CUPS (May 22, 2018), https://www.7cups.com/Documents/PrivacyPolicy/. Forty-seven percent of these apps' privacy policies (9 of 19 apps) stated that continued use of the app after the changes means that the user accepts any changes to the privacy policy, but only 16% (3 of 19 apps) specified when the changes would take effect.

93. *See Privacy Policy*, *supra* note 90.

94. The percentage of apps with privacy policies has been studied by other researchers for diabetes and blood pressure (19%) and asthma (36%). An analysis of 154 Android diabetes and blood pressure apps available in November 2014 found that only 19% of the apps provided a privacy policy. KNORR ET AL., *supra* note 83. An analysis of asthma apps in June, July, and August 2013 found that the number of asthma apps with privacy policies increased but still remained considerably low—of 92 apps, only 36% had a privacy policy. Huckvale et al., *supra* note 83.

95. For example, a Privacy Rights Clearinghouse study of health and fitness apps found that only 43% of the free apps and 25% of the paid apps provided any kind of link to the privacy policy from within the app itself. ACKERMAN, *supra* note 81, at 19. A German study of 60 free health and fitness apps available on Google Play found that only 37% (22 of 60) of health and fitness apps had active privacy policies. Three of these privacy policies did not directly relate to the app, leaving only 32% of apps with relevant privacy policies (19 of 60 apps). *Simply App-alling! Users Pay a High Price to Use Free Ehealth Apps!*, AV-TEST (Apr. 12, 2017), https://www.av-test.org/en/news/news-single-view/simply-app-alling-users-pay-a-high-price-to-use-free-ehealth-apps/.

the app specifically and instead focused on a developer homepage, all developer services, or subject matter not pertinent to the app.[96]

Like our studies, other researchers found that privacy policies are not readily understandable and may deliberately obfuscate what is being done with the user's information. A study of the privacy policies of 20 popular health and fitness apps found that the policies were at a much higher reading level and much longer than suggested for readability by the general public.[97] Researchers Joseph Bonneau and Sören Preibusch similarly found deliberate obfuscation in the language of social network sites' privacy policies, which might provide a false comfort for the users of apps who do not realize how limited the protections really are.[98] As a Silicon Valley journalist notes, "the tech industry is flush with companies that hide unsavory practices behind impenetrable terms of service agreements."[99] Thus, consumers generally do not have an adequate opportunity to assess

96. Ali Sunyaev et al., *Availability and Quality of Mobile Health App Privacy Policies*, 22 J. AM. MED. INFO. ASS'N 1, 5–6 (2014).

97. Mark Rowan & Josh Dehlinger, *A Privacy Policy Comparison of Health and Fitness Related Mobile Applications*, 37 PROCEDIA COMPUTER SCI. 348, 351–54 (2014). A similar study of 50 heavily-used websites such as Amazon and Expedia determined that websites had obscured the data collection and sharing policies with conditional or mitigating language. *See supra* text accompanying notes 87–88. For example, privacy policies were found to frequently hedge claims using terms such as "may," "might," and "we reserve the right to." Irene Pollach, *What's Wrong with Online Privacy Policies?*, 50 COMM. ACM 103, 106–07 (2007). We found similar terminology used in the privacy policies we examined in the ISLAT studies. For example, the privacy policy of Musings of a Bipolar Hot Mess stated that "E-commerce Providers may be collecting additional information regarding your interactions with their systems. For information about their privacy practices, refer to their privacy policies." By using the term "may," the reader does not know whether or not the app actually has e-commerce providers accessing their information. Ginger.io's privacy policy states, "We will not sell or use your Personal Information for purposes other than what is authorized pursuant to your End User License Agreement." *Ginger.io Emotional Support*, *supra* note 80. But the circumstances under which data and personal information could be sold are not discussed in detail in the privacy policy, so this language actually does not tell the user about Ginger.io's practices in regards to selling user data, despite seeming to do so.

98. 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, ECONOMICS OF INFORMATION SECURITY AND PRIVACY 121–68 (Tyler Moore et al. eds., 2010) (arguing that websites specifically make their privacy policies difficult to read so that users do not know what privacy is offered). Similarly, 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* Rowan & Dehlinger, *supra* note 97, at 354.

99. Nick Statt, *HBO's Silicon Valley Wades into a Heated Debate About Privacy Policies*, THE VERGE (May 1, 2017), https://www.theverge.com/2017/5/1/15504692/hbo-silicon-valley-season-4-episode-2-terms-of-service-recap.

the type of information that will be collected and shared about them before they download a health app.

C. *Did the Apps with Privacy Policies Actually Protect Privacy?*

We took various approaches to determine if the medical apps we analyzed protected privacy. We assessed whether the provisions of the privacy policies said that the app used tracking mechanisms, such as cookies and web beacons, to collect information from the app or from elsewhere on the person's phone.[100] We also assessed what the provisions were with respect to the dissemination of the information to third parties.[101]

A substantial portion of the medical apps we analyzed in the ISLAT studies stated in their privacy policies that they used tracking mechanisms. The privacy policies of 49% of diabetes apps said that they used cookies.[102] The privacy policies of 91% of the bipolar apps similarly said they used tracking technologies to acquire user data.[103]

The apps' privacy policies said they shared information in various situations: 7% of diabetes apps' policies and 5% of bipolar apps' policies said they shared the user's personal information with advertisers and, in seemingly inconsistent provisions, 39% of diabetes apps' policies indicated that user data may be used for advertisements.[104] Our subsequent transmission studies, however, found that indeed a much higher proportion of apps—a majority of apps—actually shared information with advertisers.[105]

Other researchers also found that apps with privacy policies do not necessarily protect privacy: A 2013 study of the 20 most popular health and fitness apps found that the apps shared data with 70 third parties, mostly advertising and analytics companies.[106] In 2014, the FTC Mobile Technology Unit assessed 12 free apps and found that they transmitted sensitive information to 76 different third parties.[107]

---

100. Cookies are small lines of code installed by web browsers or apps onto a computer that allow the developer to track the user's activity, while web beacons are small, invisible graphic images placed on websites, emails, or apps that can upload user information to a developer's server when the web beacon is downloaded.

101. *See infra* Table 2.

102. Yet only 31.7% let the user opt out. Blenner et al., *Privacy Policies of Android Diabetes Apps and Sharing of Health Information*, 315 J. AM. MED. ASS'N 1051, 1051 (2016).

103. *See infra* Table 2.

104. *See infra* Table 3.

105. *See infra* Subpart II.E.

106. Andy Kahl, *A Healthy Data Set*, EVIDON (Sept. 2, 2013), http://web.archive.org/web/20131005072835/http://www.evidon.com:80/blog/healthy-data-set.

107. JAH-JUIN HO ET AL., FED. TRADE COMM'N, A SNAPSHOT OF DATA SHARING BY SELECT HEALTH AND FITNESS APPS: FTC STAFF'S PRELIMINARY OBSERVATIONS 35 (2014),

D. *The Significance of Permissions*

In addition to analyzing the privacy policies of the diabetes, bipolar, eating disorder, and suicide prevention apps in the ISLAT study, we also analyzed their permissions.[108] On Google Play, each app has a list of permissions which are granted to the developer when the user downloads the app on a mobile device.[109] Permissions authorize app developers to access sensitive information, such as the ability to track the user's location (18% of diabetes apps), record audio (4%), read contacts on the phone (6%), and take pictures (11%).[110] The permissions for bipolar apps in our study included finding accounts on the device (25%), reading the user's contacts (8%), seeing their precise location (17%), modifying or editing the contents of the phone's USB storage (62%), recording audio (5%), and taking pictures or videos (13%).[111]

App permission descriptions are typically confusing and unclear[112] and the majority of Android users do not understand Android permissions.[113] Permissions are sometimes incomprehensible even to security experts.[114] Moreover, most users ignore permission disclosures when downloading and installing apps.[115] In a survey of 99 adult U.S. smartphone users, only 25% of respondents reported paying attention to permissions.[116]

Permissions have serious consequences for user privacy. Studies of permissions—including our own study—indicate that many apps are "overprivileged"—designed in an overreaching way that allow them to access, store, and share more information and undertake

---

https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf.

108. *See infra* Table 4.

109. *See Permissions Overview*, ANDROID DEVELOPERS, https://developer.android.com/guide/topics/permissions/index.html (last visited Aug. 10, 2018).

110. *See infra* Table 4.

111. *See infra* Table 4.

112. *See* Jina Kang et al., *Analyzing Unnecessary Permissions Requested by Android Apps Based on Users' Opinions*, *in* INFORMATION SECURITY APPLICATIONS 68, 68 (2014).

113. *See Privacy as Part of the App-Decision Making Process*, *supra* note 89, at 3401.

114. *See* Kang et al., *supra* note 112, at 69; ADRIENNE PORTER FELT ET AL., ANDROID PERMISSIONS DEMYSTIFIED 627–28 (2011), https://people.eecs.berkeley.edu/~dawnsong/papers/2011%20Android%20permissions%20demystified.pdf; ADRIENNE PORTER FELT ET AL., THE EFFECTIVENESS OF APPLICATION PERMISSIONS 1 (2011), https://people.eecs.berkeley.edu/~daw/papers/perms-webapps11.pdf.

115. *See* FELT ET AL., *supra* note 89 (finding in two studies that only 17% of 332 Android users paid attention to permissions during installation); *Privacy as Part of the App-Decision Making Process.*, *supra* note 89, at 3398 (finding that participants only looked at the permissions screen for an average of 3.19 seconds when trying to complete a privacy facts checklist, despite the wealth of information in the permissions).

116. Kang et al., *supra* note 112, at 73.

more functions than are necessary for the app to fulfill its stated purpose.[117] Especially when the number of overprivileged apps is so high,[118] permissions present a major risk to the privacy and security of users' personal information and even, potentially, their physical security. Of the apps whose permissions indicated that they tracked location, that fact was generally not disclosed to the user.[119]

One of the most troubling examples in our study was a diabetes app whose only function was to display recipes.[120] The permissions allowed the app to do the following: find user accounts on the phone; read and modify contacts; read the calendar; track the user's precise (GPS-based) location; make phone calls; read and modify the call log; test access to and modify external storage; obtain the device ID; activate the camera and microphone, and install and delete other applications.[121]

These permissions go well beyond any relevant purpose of the app. But the information collected through the app can be a goldmine to the developer if sold for marketing purposes. Information collected through the microphone can tell if the user eats in restaurants or at home, what television shows she watches, where she shops, and if she has sex with someone of the opposite sex or the same sex.[122]

Studies by other researchers also found overreaching permissions. A study of 940 Android apps found that about one-third of the apps had more permissions than were needed for the app to actually provide the service it purported to provide.[123] Particularly problematic is the apps' collection and storage of location data. In a 2015 Carnegie Mellon study, researchers found that ten common

117. The authors of one study found that Android apps on average had more permissions than are actually necessary to run the app. In that study, consumers objected to the overreaching permissions once they were aware of them. *See* Kang et al., *supra* note 112, at 73. The authors noted that: "a malicious app that has requested for the camera permission could silently take pictures or record videos of private moments and transfer them over the air." *See id.* at 75; Roman Schlegel et al., *Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones*, IND. UNIV. BLOOMINGTON, https://www.cs.indiana.edu/~kapadia/papers/soundcomber-ndss11.pdf (last visited Aug. 10, 2018). Also, new apps are more likely to have fewer permissions than older apps that have gone through several updates. *See* Kang et al., *supra* note 112, at 78–79. Developers disclose few permissions in original releases, but add more (often unnecessary) permissions gradually through app updates. *See id.*

118. *See* FELT ET AL., *supra* note 114, at 628–29.

119. *See infra* Table 5.

120. The app referred to here is "Diabetic Recipes Volume 1" by ECI.

121. *See id.*

122. *See* Mike Elgan, *Snooping: It's Not a Crime, It's a Feature*, COMPUTERWORLD (Apr. 16, 2011), https://www.computerworld.com/article/2507554/data-privacy/snooping—it-s-not-a-crime—it-s-a-feature.html; Will Greenwald, *Intonow's Soundprint Technology Knows What You're Watching*, PCMAG (Jan. 31, 2011), http://www.pcmag.com/article2/0,2817,2376891,00.asp.

123. FELT ET AL., *supra* note 114, at 637.

smartphone apps sent out the user's location more than five thousand times in two weeks.[124]

In an analysis of 100 paid and 856 free apps, there was a significant disparity between free and paid apps in the frequency of requests for "dangerous" permissions, defined by the researchers as permissions that control access to potentially harmful actions like sending text messages or spending money.[125] The researchers in a study of ninety-nine adult smartphone users similarly found that free apps include more unnecessary permissions than paid apps.[126] Furthermore, the free apps' permissions frequently allow for collection of personal information.[127] The researchers in that study attribute free apps' proportion of permissions which give access to personal information to their reliance on advertisements as their primary source of profit.[128] In some instances, these apps are really just acting as data collectors.

E. What Did the Apps Actually Do With Information?

For a subset of diabetes and bipolar apps, we dug deeper and assessed what the apps actually did with the information that was entered into them. We also analyzed what happened to additional information that was otherwise collected by the app, such as through passive collection of information about the user (including GPS location) or collection of other information about the user from the user's phone (such as information about contacts or the user's web searches). In combination, Charles Proxy,[129] Wireshark,[130]

---

124. Hazim Almuhimedi et al., *Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging*, CARNEGIE MELLON UNIV. SCH. OF COMPUTER SCI., http://www.cs.cmu.edu/~halmuhim/MobileAppPrivacyNudging_CHI2015.pdf (last visited Aug. 10, 2018); Byron Spice, *Carnegie Mellon Study Shows People Act to Protect Privacy When Told How Often Phone Apps Share Personal Information*, CARNEGIE MELLON UNIV. SCH. OF COMPUTER SCI. (Mar. 23, 2015), http://www.cs.cmu.edu/news/carnegie-mellon-study-shows-people-act-protect-privacy-when-told-how-often-phone-apps-share-personal-information.

125. FELT ET AL., *supra* note 89, at 5–6.

126. Kang et al., *supra* note 112, at 76.

127. *See id.* at 78.

128. *See id.*

129. Charles Proxy is an internet proxy server that acts as an intermediary between a device that attempts to communicate via the internet and the internet itself. By configuring Charles Proxy software on a laptop and connecting the test Android smartphone to the laptop via Wi-Fi, ISLAT researchers were able to gather specific internet destinations for all of the traffic that the observed diabetes and psychiatric apps sent out to the internet and could examine what specific data was being sent in most cases, all without the apps themselves being aware that they were being monitored. *Charles: Web Debugging Proxy Application*, CHARLES PROXY, http://www.charlesproxy.com/ (last visited Aug. 10, 2018).

130. Wireshark is desktop computer software that intercepts all internet network traffic for the user to see what information is transmitted unencrypted on the network. ISLAT researchers used Wireshark to determine what

Cygwin,[131] and Wakelock Detector[132] allowed us to intercept all outgoing and incoming transmissions, decrypt lightly encrypted transmissions, and determine what programs the app ran on the device.

In our diabetes app study, many apps with privacy policies did not protect privacy but instead disclosed sensitive information to unrelated entities. We analyzed the digital trails of 65 apps out of the 211 total diabetes apps. Twenty-four of these 65 apps had privacy policies while the other 41 did not.[133] Of the 65-app subset, 86% placed cookies on the user's device.[134] Apps with privacy policies were no more protective of privacy than apps without them. In fact, 79% of diabetes apps with privacy policies disclosed information to third parties,[135] a slightly higher amount than the 76% of those without privacy policies.[136]

In our bipolar app study, out of the 26-app subset whose transmissions we analyzed, 69% shared information with advertising networks or data analytics companies.[137] Fifty percent of these apps sent information to the data aggregator DoubleClick.[138] Sixty-two percent of apps sent data to their developer's server, and many apps sent information to other third parties.[139]

---

information the diabetes and psychiatric apps transmitted in plain text from the test Android smartphone and were thus vulnerable to network snooping. *About Wireshark*, WIRESHARK, https://www.wireshark.org/ (last visited Aug. 10, 2018).

131. Cygwin is desktop computer software that uses Android Debugging Bridge commands to determine what files an app runs on an Android device. ISLAT researchers used Cygwin to collect files regarding the functions that the psychiatric apps ran on the test Android smartphone. *This is the Home of the Cygwin Project*, CYGWIN, https://www.cygwin.com/ (last visited Aug. 10, 2018, 2018). The diabetes app study used a similar program, Android Debug Bridge, to determine what files the diabetes apps ran on the test Android smartphone. *See Android Debug Bridge (adb)*, ANDROID DEVELOPERS, https://developer.android.com/tools/help/adb.html (last visited Aug. 10, 2018).

132. Wakelock Detector is an Android app that allows the user to monitor screen and CPU access by different apps on an Android smartphone, even when the apps are no longer opened by the user. ISLAT researchers used Wakelock Detector on the Android test smartphone to determine how the psychiatric apps accessed the smartphone's screen and CPU. Wakelock Detector was not used for the diabetes app study. *Wakelock Detector [Root]*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.uzumapps.wakelockdetector&hl=en (last visited Aug. 10, 2018).

133. Blenner et al. *supra* note 102.

134. *Id.*

135. *Id.*

136. *Id.* For example, 15 diabetes tracking apps transmitted data from the app to data aggregator DoubleClick. Four diabetes tracking apps transmitted data to non-Google affiliated marketers.

137. *Id.*

138. *Id.*

139. *Id.*

Another threat to the user's privacy comes from apps failing to encrypt the data the apps transmitted.[140] We found that not all the apps stored or sent information encrypted. In our bipolar app transmissions study, only 42% of the apps encrypted transmissions.[141] One app, MoodPanda,[142] sent out the user's password unencrypted. Considering that people use the same password for multiple purposes, this is particularly problematic. RxWiki transmitted unencrypted information about the user's medication searches to seven different URLs related to Google, Google Analytics, DoubleClick, and Facebook,[143] allowing not only these sites to know about the searches the app user conducted, but also any network snoopers. In one case, even though the privacy policy stated that the user's personal information was encrypted, the app still sent an unencrypted transmission containing the user's email address and a list of all the other applications installed on the phone at the time.[144]

Other studies similarly found that apps failed to encrypt information.[145] The Privacy Rights Clearinghouse commissioned a study of health and fitness apps that found that only 10% of paid apps encrypted all of the data connections and transmissions to and from the app and the developer.[146]

III. CREATING A FRAMEWORK FOR PROTECTION OF INFORMATION FROM MEDICAL APPS

A. *The Rationale for the Protection of Health Information*

Health information in the hands of health care providers is protected for two reasons: so that patients get appropriate care by being honest with their doctors and so they will not be discriminated against based on their health status.[147] Those same concerns exist in the online world. People are reluctant to disclose health information when they find out how vulnerable it is online, even in situations

140. *See infra* Table 7.

141. *See id.*

142. MOODPANDA, http://moodpanda.com/ (last visited Aug. 19, 2018).

143. *Mobile Apps*, RXWIKI (Nov. 20, 2013), https://www.rxwiki.com/mobile/apps.

144. *Privacy Policy*, MOODLYTICS, http://www.moodlytics.com/privacy-policy (last visited Aug. 10, 2018). Other apps failed to encrypt information saved on the phone. For example, in the diabetes study, although all apps used at least some encryption for data in transit, only one app encrypted data on the phone. *See Diabetes Pharma*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=red.ebersalud&hl=en (last visited Aug. 10, 2018).

145. *See id.*

146. In addition, they found that 39% of free apps and 30% of paid apps transmitted user data to an unknown party. Only 11.63% of health and fitness apps encrypted all transmissions that were sent out. ACKERMAN, *supra* note 81, at 19.

147. *See id.*

where disclosure could help them. Concerns about privacy deter some people from obtaining a medical app, which can prevent them from gaining much needed control over the management of their health.[148] And discrimination can flourish when health information from medical apps is sold. If someone uses a bipolar or diabetes app and her information is disclosed to potential employers, she might be turned down for a job interview and never find out why.

Our studies identified problematic practices that merit a legal response. These include: lack of privacy policy (thus failing to provide notice to the user about how the apps will collect and disseminate information), collection of information in privacy-invading ways (such as by turning on a microphone), dissemination of health or other private information, dissemination of information that is linked to health but is not traditionally considered health information (such as gait), and dissemination of information without encryption.

Even though health information is an extremely sensitive category of information and people generally think of it as highly protected, existing federal regulations fall short. Existing federal regulations such as HIPAA, the regulations about misrepresentation and unfair business under the Federal Trade Commission Act, federal law concerning digital data, and state privacy torts fall short in various ways when it comes to protecting the information collected by medical apps.[149]

B. Existing Protections Under HIPAA and Their Possible Expansion

When doctors collect information about their patients, a wide range of ethical and legal protections assure that the information is kept confidential. The Hippocratic Oath,[150] the American Medical Association Code of Ethics,[151] and other ethical precepts that guide doctors start from the premise that they must keep patient information confidential. State medical codes[152] also protect patient

148. Studies of consumers indicate that for some, privacy is a concern in whether to buy or continue to use a particular health app. In a 2012 study of 60 U.S. adults, participants were less willing to access health data on their mobile phone than on their laptop. Of 19 participants who were not willing to use "health document services" on their mobile phone, 47% (9) cited security reasons. ERIKA CHIN ET AL., MEASURING USER CONFIDENCE IN SMARTPHONE SECURITY AND PRIVACY 5 (2012). In a 2012 Blue Chip Patient Recruitment survey of 705 smartphone-owning patients aged 35 years and older with at least one health condition, 45% of the patients reported having privacy concerns when using their mobile device for health-related activities. *See* BLUE CHIP PATIENT RECRUITMENT, LEVERAGING MOBILE HEALTH TECHNOLOGY FOR PATIENT RECRUITMENT: AN EMERGING OPPORTUNITY 9 (2012).

149. *See infra* Subparts III.B–III.D.

150. *See Hippocratic Oath*, *supra* note 36.

151. *See AMA Code of Medical Ethics: AMA Principles of Medical Ethics*, *supra* note 37.

152. *See, e.g.*, Medical Practice Act of 1987, 225 ILL. COMP. STAT. 60/22 (1987).

confidentiality and contain penalties for disclosure that include probations, fines, and loss of the doctor's medical license.[153] State law causes of action, including public disclosure of private facts,[154] fiduciary duty law,[155] malpractice,[156] contract,[157] and warranty law,[158] as well as state statutes governing health care privacy,[159] also provide ways to hold doctors accountable when they disclose patient information.

Within that thicket of privacy protections, the federal regulations adopted pursuant to HIPAA provide an additional narrow strand of protection. The regulations require that patients be given advance notice about the privacy practices of their physicians and other health care providers.[160] They also require that consent be sought from patients before their information is shared with certain third parties such as insurers and researchers[161] and that adequate data security practices be used when information is digitally transmitted.[162] Even though HIPAA protects health information in the hands of health care professionals and health care institutions, it does not apply to user-generated data from medical apps.[163] Nor does it cover information that is not traditionally considered health information (such as GPS information or gait) that could nonetheless be used to discriminate against a person because of its true or even erroneous association with a health condition.

Additionally, HIPAA is an administrative protection. It contains no provision for a private cause of action.[164] Its focus is more on uniformity of disclosure and consent procedures than on true protection of patient information. This works with respect to information in the hands of doctors because the context of medical practice provides other heightened protections, as well as a way for aggrieved individuals to bring lawsuits.[165]

Some states have extended HIPAA-like protections to digital entities[166] in ways that could include medical apps. However, because

---

153. *See, e.g.*, *id.* 60/22 (A)(30).
154. *See* Horne v. Patton, 287 So.2d 824, 830–31 (Ala. 1973).
155. *See id.* at 828.
156. *See* MacDonald v. Clinger, 84 A.D.2d 482, 488–89 (N.Y. App. Div. 1982) (Simons, J., concurring).
157. *See Horne*, 287 So.2d at 824.
158. *See* Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793, 801 (N.D. Ohio 1965).
159. *See id.*
160. *See* Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.520 (2018); *see also id.* § 164.502.
161. *See id.* § 164.508.
162. *See id.* § 164.312(e).
163. *See id.* § 160.103.
164. *See* Acara v. Bans, 470 F.3d 569, 571 (5th Cir. 2006).
165. *See id.*
166. *See, e.g.*, TEX. HEALTH AND SAFETY CODE ANN. § 181.00(b) (West 2018); CAL. CIV. CODE §§ 56–59 (West 2018).

of the failure to understand the legal context of the physician-patient relationship and the unique nature and scope of medical app information, these statutes do not provide adequate protection to app users.

Texas, for example, expands HIPAA's definition of a covered entity to include other entities that collect protected health information.[167] It forbids such an entity from disclosing protected health information (other than, say, to insurers) in exchange for direct or indirect remuneration.[168] Like HIPAA, though, it only covers information that is traditionally considered to be health information.[169] It allows the marketing of a person's information as long as that person's consent is obtained.[170] Also, the penalties within the statute—fines[171] and potential exclusion from state-funded health care programs[172]—do not compensate the person whose information has been disclosed.[173]

A California statute[174] also attempts to extend HIPAA-like protection to more entities. California's law requires that any business that offers software or hardware that is designed "for purposes of allowing the individual to manage her information, or for the diagnosis, treatment, or management of a medical condition of the individual shall be deemed a provider of health care,"[175] and must maintain "the same standards of confidentiality required of a provider of health care."[176] The statute explicitly states, though, that other protections of confidentiality in the physician-patient relationship do not apply.[177]

Although the California statute seems broad and allows for civil suits with statutory damages,[178] the type of information that is covered is extremely limited. The statute only protects identifiable medical information "in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment."[179] While this could be interpreted to protect

167. *See* TEX. HEALTH & SAFETY CODE ANN. § 181.001(b).
168. *See id.* § 181.153(a).
169. *See id.*
170. Private health information may not be used, disclosed, or sold for marketing purposes without first obtaining "clear and unambiguous permission in written or electronic form" from the consumer. *See id.* § 181.152(a). It is unclear whether clicking "I agree" in a clickwrap agreement would qualify as clear and unambiguous.
171. *See id.* § 181.201.
172. *See id.* § 181.203.
173. *See id.*
174. *See* CAL. CIV. CODE § 56.06 (West 2018).
175. *See id.* § 56.06(b).
176. *See id.* § 56.06(c).
177. *See id.* § 56.06(b).
178. *See id.* §§ 56.35–56.36.
179. *See id.* § 56.05(j).

user-generated information from medical apps in the hands of the app developers (as a provider of health care), some app developers disavow that they are providing health care or medical advice but are for "entertainment purposes" only.[180] In addition, making the app developer liable would not protect the information in the hands of data aggregators that obtained it with cookies from other apps or search engines. It seems that the statute was designed to cover information that was protected by HIPAA in the doctor's hands when that doctor shares the information via an app with a patient. A strict reading of that provision would mean that user-generated information or data collected passively by a medical app would not be protected.[181] Also, since the statute protects only medical information, the law would not protect the user from breaches of privacy based on information that may predict a health status (such as gait information) that the individual is not using to assess her health, but which could be used by others to assess her health. Nor would it protect GPS information showing a person is at a health care provider's office where the recipient of such information uses it as evidence the person is ill with no way of knowing if the person was just aiding someone else at the clinic.

C. The Federal Trade Commission

The FTC is directed, under Section 5 of the Federal Trade Commission Act, to prevent "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[182] These include any act or practice which "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[183]

A variety of practices that we found in our studies could be addressed as unfair or deceptive trade practices by the FTC, including failure to disclose that an app will be disseminating information to

180. For example, Undercover Scientists' iStethoscope Pro is a mobile health app that helps the user listen to heartbeats and view the accompanying heartwave form with phonocardiograph and spectrogram capabilities. *Istethoscope Pro: Listen to Quiet Sounds Around You*, UNDERCOVER SCIENTIST, http://www.peterjbentley.com/istethoscopepro.html (last visited Aug. 10, 2018). However, the description on the App Store says that the app is for entertainment use only. *Istethoscope Pro*, APPLE ITUNES, https://itunes.apple.com/us/app/istethoscope-pro/id322110006?mt=8 (last visited Aug. 10, 2018).

181. *See id.*

182. *See* 15 U.S.C. § 45(a)(1) (2012).

183. *See id.* § 45(n). In addition to this enforcement authority, the FTC has a Mobile Technology Unit that performs research, marketplace monitoring, and internal staff training on issues related to mobile devices. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 4 (2013), http://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission.

third parties or collecting GPS information.[184] In our studies of medical apps, we found apps that shared information without adequate notice to the users. This included 76% of diabetes apps without privacy policies which routinely disseminate information to third parties.[185] In an analogous instance, *FTC v. Frostwire, LLC*,[186] the FTC settlement barred a company from "using default settings likely to cause inadvertent public sharing of files by consumers" and required "clear and prominent disclosures about file sharing and how to disable it."[187]

The FTC could bring actions against app developers for sharing a user's location without the user's knowledge.[188] Fifteen percent of diabetes apps and 24% of psychiatric apps had access to the user's precise location.[189] In an analogous instance, the FTC settled with Goldenshores Technologies, LLC, the maker of Brightest Flashlight Free, an Android app with tens of millions of downloads, over its undisclosed collection and sharing of users' geolocation information.[190] According to the FTC, the app's privacy policy "deceptively failed to disclose that the app transmitted users' precise location and unique device identifier to third parties, including advertising networks."[191] The settlement required the company to obtain express consent before collecting users' geolocation

184. *See id.* at 12–13.

185. Blenner et al., *supra* note 102.

186. No. 1:11-cv-23643 (S.D. Fla. Oct. 7, 2011).

187. *See Peer to Peer File-Sharing Software Developer Settles FTC Charges*, FED. TRADE COMM'N (Oct. 11, 2011), https://www.ftc.gov/news-events/press-releases/2011/10/peer-peer-file-sharing-software-developer-settles-ftc-charges. The FTC alleged that Frostwire's file sharing app was unlawful because it misrepresented how downloaded files were shared, and because its unfair design was likely to cause a significant number of consumers to unwittingly share files stored on their mobile devices. Stipulated Final Order, Fed. Trade Comm'n v. Frostwire LLC, et al., No. 11-23643-CV-GRAHAM, at 5 (S.D. Fla. Oct. 12, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111012frostwirestip.pdf.

188. *See Privacy & Data Security Update*, FED. TRADE COMM'N (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016.

189. *See infra* Table 4.

190. *See Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, FED. TRADE COMM'N (Dec. 5, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived; *see also* Agreement Containing Consent Order, In the Matter of Goldenshores Techs., LLC, No. 132-3087, at 4, https://www.ftc.gov/sites/default/files/documents/cases/131205goldenshoresorder.pdf [hereinafter *Goldenshores Agreement Containing Consent Order*].

191. *See Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, *supra* note 189. Furthermore, the app began collecting and transmitting location data and the unique device identifier even before the user could accept or reject the end-user license agreement. The FTC alleged that these behaviors constituted unfair or deceptive acts or practices in or affecting commerce violating Section 5(a) of the FTC Act. *See Goldenshores Agreement Containing Consent Order*, *supra* note 189, at 3–4.

information and fully disclose the purpose and use of the information before requesting consent.[192]

The FTC could launch investigations into other egregious practices of medical apps we uncovered in our studies. However, the FTC generally has chosen to take action only when an app developer fails to disclose in advance that it will be invading a person's privacy.[193] If an app developer states in advance that it will be collecting and sharing a person's information, the FTC cannot argue that the developer misrepresented its practices. Given that people rarely read privacy policies[194] and that most are overreaching or deliberately confusing, the FTC's actions requiring disclosure do not adequately protect medical app users. Advance disclosures will not protect users from having sensitive information that is actively or passively collected by medical apps from being disseminated to their detriment.

D. Existing Protection Under State Tort Laws and Their Possible Expansion

The collection and dissemination of information by medical apps might give rise to conventional tort causes of action such as intrusion on seclusion, public disclosure of private facts, false light, or unjust enrichment.[195] However, these causes of action have limitations and would not cover all of the abuses that we, and others, have uncovered in studies of medical apps. For example, some of the privacy tort actions could fail because the disclosure is not "public" enough,[196] even though disclosure might be harmful to the app user, such as if the disclosure was made to a potential insurer or employer. These actions may also fail based on a defense that the individual explicitly or implicitly consented to the disclosure when the app offered a privacy statement or permission that forewarned of disclosure.[197] Still other causes of action might be impeded if the information that is disclosed is not considered "offensive" enough[198] (even though such disclosure might be harmful to the user, as in the case when gait

192. *See Goldenshores Agreement Containing Consent Order*, *supra* note 189.

193. *See, e.g.*, *PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act*, FED. TRADE COMM'N (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

194. *See* GLOBAL INTERNET USER SURVEY SUMMARY REPORT, INTERNET SOCIETY 1, 4 (2012), http://wayback.archive-it.org/9367/20170907075228/https://www.internetsociety.org/sites/default/files/rep-GIUS2012global-201211-en.pdf.

195. *See infra* Subpart III.D; *see also* Alexander H. Tran, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J.L. & SOC. PROBS. 263, 263 (2017).

196. *See infra* Subparts III.D.2–III.D.3.

197. *See infra* Subparts III.D.1–III.D.4.

198. *See infra* Subparts III.D.2–III.D.3.

information is shared with an insurer or nursing home). Moreover, the user would have to learn that the harmful disclosure had come from an app, and given the hidden aspects of the collection, transmission, and sale of medical app data, these linkages will undoubtedly be very difficult to document to support legal claims. While judges have discretion to interpret invasion of privacy broadly,[199] that result is not guaranteed; thus, these existing tort doctrines have substantial shortcomings for dealing with the problems associated with apps.

1. Intrusion on Seclusion

Information collection by medical apps may, in certain instances, qualify as an intrusion on seclusion. The tort of intrusion on seclusion requires that a party intentionally intrude, physically or otherwise, upon the solitude of another or her private affairs or concerns in a manner that would be highly offensive to a reasonable person.[200] Liability exists for the intrusion itself and does not require the dissemination of the information.[201]

The information collected through the intrusion need not be offensive. However, the nature of the intrusion itself must entail offensive conduct to which a reasonable person would strongly object.[202] This includes, for example, peeping into a person's window[203] or secretly taping her conversation.[204] It also includes an investigation of the plaintiff's private concerns, such as opening mail, searching a wallet, examining a bank account, or inspecting personal documents[205]—but does not include examination of public records.[206]

The tort of intrusion on seclusion has limits, however. It does not apply when someone has consented to the intrusion,[207] even under a broad consent that does not specify that health care information will be collected.[208] Nor does it apply when an entity uses information from its own files. For example, in a case involving intrusion on seclusion, the plaintiffs accused the defendant, TransUnion, of accessing, disclosing, and selling private financial, credit, and other

199. This has happened, for example, when judges interpret the public disclosure of private facts cause of action to apply even without disclosure to the public at large. *See infra* Subpart III.D.2.

200. RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

201. *See In re* TransUnion Corp. Privacy Litig., 326 F. Supp. 2d 893, 901 (N.D. Ill. 2004); Corcoran v. Southwestern Bell Telephone Co., 572 S.W.2d 212, 215 (Mo. App. 1978); RESTATEMENT (SECOND) OF TORTS § 652B cmt. a.

202. *See* RESTATEMENT (SECOND) OF TORTS § 652B.

203. *See id.* § 652B cmt. b.

204. *See* McDaniel v. Atlanta Coca-Cola Bottling Co., 2 S.E.2d 810, 816 (Ga. Ct. App. 1939); Hamberger v. Eastman, 206 A.2d 239, 241 (N.H. 1964); Roach v. Harper, 105 S.E.2d 564, 566 (W. Va. 1958).

205. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b.

206. *See id.* § 652B cmt. c.

207. *See* Vespa v. Safety Fed. Savings & Loan Ass'n, 549 P.2d 878, 881 (1976).

208. *See* Smith v. Facebook, Inc., 262 F. Supp.3d 943, 953 (N.D. Cal. 2016).

confidential information without the plaintiffs' knowledge, authority, or consent.[209] Since it is the intrusion that creates liability and not subsequent publication or disclosure, TransUnion successfully argued there can be no unlawful intrusion when a company accesses its own lawfully obtained files.[210]

In our studies, it could be argued that the apps that turn on a smartphone's microphone (6% of diabetes apps; 4% of bipolar apps) or camera (9% of diabetes apps; 12% of bipolar apps) or that access GPS information (29% of diabetes apps; 19% of bipolar apps) intrude upon seclusion.[211] Perhaps even the collection of information beyond that needed for the functions of the app would be considered intrusion on seclusion, akin to taping someone's conversation. Similarly, the use of tracking mechanisms such as cookies and web beacons (as described in the privacy statements of 49% of diabetes apps and 59% of psychiatric apps and actually used in 86% of the diabetes apps) could be actionable, much as the landlord's bugging of an apartment is, even if the data is not disseminated to third parties.[212]

There would be challenges, however, to asserting an intrusion on seclusion claim. The collection of GPS information, which indicates someone is in a public place, might not be considered an intrusion on seclusion,[213] even if that public place is a fast food restaurant (a fact which can be used against someone seeking life insurance).[214] And the sale of even highly sensitive information to a data aggregator from the app developer's records may be considered permissible under the

209. *See In re* TransUnion Corp. Privacy Litig., 326 F. Supp. 2d 893, 901 (N.D. Ill. 2004).

210. *See id.* at 901; *see, e.g.*, Dwyer v. American Express Co., 652 N.E.2d 1351, 1355 (Ill. App. 1995) (concluding no intrusion upon seclusion when defendant accessed its own files).

211. Other tracking in the app may also be construed as intrusion upon seclusion, such as the apps that "create accounts and set passwords," in the permissions of 2 apps in our diabetes app study and 2 apps in our psychiatric app study, "find accounts on the device," in the permissions of 30 apps in our diabetes app study and 32 apps in our psychiatric app study, and "use accounts on the device," in the permissions of 4 apps in our diabetes app study and 6 apps in our psychiatric app study. These permissions give apps access to information that can be used to easily identify users ("*e.g.*, emails, Facebook accounts, etc."), according to a study of Android privacy risks. *See* Alexios Mylonas et al., *Assessing Privacy Risks in Android: A User-Centric Approach*, *in* RISK ASSESSMENT AND RISK-DRIVEN TESTING 22-24 (Thomas Bauer et al., eds. 2013). One of the permissions disclosed by the diabetes and psychiatric apps in the ISLAT study ("read phone status and identity") gives apps access to information that has a strong correlation with user identity according to the same study ("*e.g.*, users[']' name or phone number").

212. *See* Hamberger v. Eastman, 206 A.2d 239, 241–42 (N.H. 1964).

213. Intrusion on seclusion does not cover observations made or photos taken while the plaintiff is on public land. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (AM. LAW INST. 1977).

214. *See* BETTY ET AL., *supra* note 59, at 4; Fitzgerald, *supra* note 59.

TransUnion precedent if the app user has given permission for its collection.[215]

2. Public Disclosure of Private Facts

While the tort of intrusion on seclusion covers the collection of information, the tort of invasion of privacy by the public disclosure of private facts concerns the dissemination of that information. The Restatement (Second) of Torts Section 652D states:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[216]

Under the Restatement, publicity "means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[217]

The hurdles in applying this cause of action to the disclosure practices of medical apps are showing that the disclosure was sufficiently public and sufficiently offensive, and that the user did not consent to the disclosure. The tort requires that the disclosure be "broadcast to the public in general or publicized to a large number of people."[218] Courts have held that the following disclosures were *not* sufficiently public to satisfy the publicity requirement: to a single person or small group of persons;[219] a "small group" of co-workers;[220] a single entity;[221] a handful of people;[222] a very small group of unidentified persons;[223] a few unidentified persons;[224] three, or a small group of prospective employers;[225] a letter to one person and an

215. *See* In re TransUnion Corp. Privacy Litig., 326 F. Supp. 2d 893, 902 (N.D. Ill. 2004).

216. RESTATEMENT (SECOND) OF TORTS § 652D.

217. *See id.* § 652D, cmt. a.

218. *See* Young v. Barker, 405 N.W.2d 395, 401 (Mich. App. 1987).

219. *See* Freeman v. Unisys Corp., 870 F. Supp. 169, 174 (E.D. Mich. 1994).

220. *See, e.g.*, Vinson v. Koch Foods of Alabama, LLC, No. 2:12-cv-1088-MEF, 2013 WL 5441969, at *7 (M.D. Ala. Sept. 27, 2013); Eddy v. Brown, 715 P.2d 74, 78 (Okla. 1986); Dietz v. Finlay Fine Jewelry Corp., 754 N.E.2d 958, 966 (Ind. Ct. App. 2001); Laronde v. Blount, No. 0831, 2015 WL 5923679, at *10 (Md. Ct. Spec. App. Aug. 17, 2015).

221. *See* Lemnah v. Am. Breeders Serv., Inc., 482 A.2d 700, 704 (1984).

222. *See, e.g.*, Green v. City of Wichita, Kan., 47 F. Supp. 2d 1273, 1279 (D. Kan. 1999); Blackthorne v. Posner, 883 F. Supp. 1443, 1456–57 (D. Or. 1995); Armstrong v. Thompson, 80 A.3d 177, 189 (D.C. 2013).

223. *See, e.g.*, Hendry v. Conner, 226 N.W.2d 921, 923 (Minn. 1975).

224. *See* Morrissey v. Nextel Retail Stores, L.L.C., Nos. 277893, 279153, 2009 WL 387750, at *3 (Mich. Ct. App. Feb. 17, 2009).

225. *See* Byington v. NBRS Fin. Bank, 903 F. Supp. 2d 342, 353 (D. Md. 2012).

email to three people;[226] two friends and a person at the gym;[227] a group of six people;[228] a group of nine people;[229] a small, discrete set of colleagues;[230] and to a "finite" group of unidentified persons.[231]

Although the general rule requires disclosure to the public,[232] the publicity element can be satisfied by disclosure of information to a small number of people who have a "special relationship" with the plaintiff, such as fellow employees,[233] club members, church members, or family.[234] Courts have realized that in circumstances where a special relationship exists between the plaintiff and the small group of individuals to whom the information is disclosed, the disclosure may be just as devastating to the individual as if it had been disclosed to the public at large.[235] These include disclosure of medical information to co-workers[236] or potential employers.[237] The rationale is that "there certainly can be 'unreasonable and serious interference' with one's privacy without everyone being informed,"[238] such as when the group consists of individuals "whose knowledge of the private facts would be embarrassing to the plaintiff."[239]

---

226. *See* L-S Indus., Inc. v. Matlack, 641 F. Supp. 2d 680, 686–88 (E.D. Tenn. 2009).

227. *See* Gleason v. Smolinski, No. NNHCV065005107S, 2012 WL 3871999, at *11, *16 (Conn. Super. Ct. Aug. 10, 2012).

228. *See* Vasquez v. Loza-Vega, No. CV126013551, 2014 WL 783820, at *6 (Conn. Super. Ct. Jan. 28, 2014).

229. *See* Grigorenko v. Pauls, 297 F. Supp.2d 446, 448–49 (D. Conn. 2003); Orsini v. Zimmer, No. CV075013711S, 2009 WL 5698148, at *7–8 (Conn. Super. Ct. Dec. 24, 2009).

230. *See* Handler v. Arends, No. 0527732S, 1995 WL 107328, at *14 (Conn. Super. Ct. Mar. 1, 1995).

231. *See* Nelson v. Nielsen Co., No. AANCV136013732, 2014 WL 2853847, at *4 (Conn. Super. Ct. May 15, 2014).

232. *See* McSurely v. McClellan, 753 F.2d 88, 112 (D.C. Cir. 1985); Young v. Barker, 405 N.W.2d 395, 401 (Mich. App. 1987).

233. *See* Pachowitz v. Ledoux, 666 N.W.2d 88, 95–97 (Wis. Ct. App. 2003).

234. *See McSurely*, 753 F.2d at 112–13.

235. In *Miller v. Motorola, Inc.*, 560 N.E.2d 900, 900 (Ill. App. Ct. 1990), an Illinois Appellate Court found a plaintiff's claim to be sufficient where her employer divulged information regarding plaintiff's mastectomy surgery to her coworkers. The court declined to follow the notion that "publicity" requires the disclosure to be widespread. *Id.* at 902. The court in *Miller* recognized that despite a general requirement for disclosure to more than a small group, there is a need for flexibility when determining whether to permit recovery under this tort. *See id.* at 903; Beaumont v. Brown, 257 N.W.2d 522, 529 (Mich. 1977) (noting there was a respectable opinion supporting the idea that "publication of the embarrassing facts to only one person alone was unlawful publication").

236. *See Miller*, 560 N.E.2d at 903 (exact number of coworkers not included).

237. *See Beaumont*, 257 N.W.2d at 523.

238. *See id.* at 531.

239. *See id.* While this is typically assessed relative to the customs of the specific time and place of each case, a defendant is liable if the disclosure is so offensive as to "shock the ordinary sense of decency or propriety." *See* Strand v. John C. Lincoln Health Network, Inc., No. CV-10-02112-PHX-NVW, 2011 WL 1253408, at *5 (D. Ariz. Mar. 31, 2011) (holding that disclosure of plaintiff's latex

In addition to demonstrating public disclosure or a special relationship, the plaintiff must show that the disclosure is of a kind that "would be highly offensive to a reasonable person."[240] The Restatement justifies this standard by explaining that "[c]omplete privacy does not exist in this world except in a desert, and anyone who is not a hermit must expect and endure the ordinary incidents of the community life of which he is a part."[241]

With respect to medical apps, the public disclosure of private facts cause of action would likely be most useful in instances where there is no privacy policy (81% of diabetes apps and 62% of psychiatric apps in our study)[242] or where a privacy policy exists but fails to disclose that the app will be sharing information with third parties, and where the information that is widely shared is clearly sensitive in nature, such as medical information (including information about legal or illegal drug use, medical condition, or treatment regimen) or highly private information (such as information about depression, suicidal thoughts, or sexual practices). If medical information or other sensitive information is disclosed to an employer or insurer, courts could find that the disclosure is "offensive" enough; even though disclosed to a single entity, the disclosure would be just as devastating to the individual as if it had been disclosed to the public at large.

The disclosure of GPS information may or may not be considered "highly offensive," even though the disclosure of such information could cause harm to an individual. The information could be used in an attack on the individual, as in the actual case of a rape based on GPS information.[243] Also, GPS information may disclose that a person is at an abortion clinic, AIDS clinic, or other medical facility. Other medical app information, such as gait information, or the types of restaurants the person eats at, also might not fall under the rubric of "offensive," even though it could be used by an insurer to the person's disadvantage.[244]

---

allergy to hospital co-workers was not highly offensive); Gill v. Hearst Pub. Co., 253 P.2d. 441, 445 (Cal. 1953); *see also* Peterson v. Moldofsky, No. 07-2603-EFM, 2009 WL 3126229, at *2 (D. Kan. Sept. 29, 2009) ("Conduct is not extreme and outrageous unless it is regarded as being beyond the bounds of decency and utterly intolerable in a civilized society."). Courts have imposed liability for dissemination of confidential medical or psychiatric information as offensive under public disclosure of private facts. *See, e.g.*, Williams v. Am. Broad. Cos. 96 F.R.D. 658, 669 (W.D. Ark. 1983) (filming of surgery); Lentz v. City of Cleveland, 410 F. Supp.2d 673, 699–701 (N.D. Ohio 2006) (finding an offensive public disclosure when a police officer's pre-employment psychological evaluations were made public as part of an investigation into an on-the-job shooting).

240. *See Peterson*, 2009 WL 3126229, at *4.

241. *See* RESTATEMENT (SECOND) OF TORTS § 652D, cmt. c (AM. LAW INST. 1977).

242. *See infra* Table 1.

243. *See* Hill, *supra* note 16.

244. *See* McFarland, *supra* note 17.

Since consent is a defense to this tort, much will depend on whether the app user implicitly or explicitly agreed to the disclosure of her information.[245] Thus, as with the federal statutory causes of action discussed previously, an app developer might be able to avoid a public disclosure of private facts suit by describing the disclosure policies in advance.

3. False Light

When a medical app conveys true information (such as the fact the user's GPS location puts her at a health care facility) in a way that creates an offensive false impression (that she is ill), there is the potential to sue under a false light claim. The Restatement states the elements for an invasion of privacy tort by publicly placing or putting a person in a false light:

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.[246]

The information disclosed does not have to be false to state a claim for false light invasion of privacy.[247]

Generally, the publicity requirement of the false light invasion of privacy claim may *not* be satisfied by communication "to a single person or even to a small group of persons."[248] For instance, in *Benson v. AJR, Inc.*,[249] an employer's disclosure of an employee's drug test results to three people, all of whom were employees, officers, or creditors of the employer, did not satisfy the widespread publicity requirement to prove a claim for false light invasion of privacy.[250]

However, courts have recognized that the special relationship rule can apply to the public disclosure requirement for this tort.[251] Persuaded by the application of the special relationship test to public

245. *See* RESTATEMENT (SECOND) OF TORTS § 652D, cmt. c.

246. *Id.* § 652E. Under the Restatement, publicity "means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." *Id.* § 652D, cmt. a. Notably, this is the same requirement as for the Public Disclosure of Private Facts Tort. *See* Doe v. TCF Bank Illinois, FSB, 707 N.E.2d 220, 221 (Ill. App. Ct. 1999).

247. *See* Larsen v. Phila. Newspapers, Inc., 543 A.2d 1181, 1189 (Pa. Super. Ct. 1998).

248. *See* Regions Bank v. Plott, 897 So. 2d 239, 245 (Ala. 2004).

249. 599 S.E.2d 747 (W. Va. 2004).

250. *See id.* at 751–52.

251. *See infra* text accompanying note 249.

disclosure of private facts cases,[252] some courts have adopted that test in the false light invasion of privacy context.[253]

In the context of medical apps, typically the user's goal is to enter accurate information so that the app can help monitor a condition or manage general health.[254] Notwithstanding circumstances where an individual may fib about her daily calorie intake or daily weight, in most cases the information a user inputs into a medical app will be true. If a medical app were to disclose that information, the plaintiff would need to be able to show that the information was improperly represented.[255] For instance, if a woman inputted information about being late in her cycle into a period tracker app, a disclosure that incorrectly represented that the woman was pregnant would place her in a false light.

This reasoning could also apply to information gathered by medical apps that the app user does not affirmatively enter. For instance, if the app were to collect information about a user's gait, the information may represent that the individual has Huntington's disease when in fact she just has the flu. Sharing this gait information then could place the user in a false light. If the app collects a person's GPS location, it may show that the user has been to a specific hospital six times in the past month. The publication of this information would imply that the individual is sick, when actually the hospital lobby might just house that individual's favorite coffee shop. Static numbers and data points are easily misinterpreted, and it is likely that medical apps that disclose or sell this information would be engaging in misrepresentation in a manner sufficient to place the app user in a false light.[256]

---

252. *See* Miller v. Motorola, Inc., 560 N.E.2d 900, 901–03 (Ill. App. Ct. 1990). The *Miller* court adopted the position that the public disclosure requirement may be satisfied by proof that the plaintiff has a special relationship with the public to whom the information is disclosed. The rationale for the rule was that the disclosure to a limited public with a special relationship may be just as devastating to the person as if it had been disclosed to the public at large.

253. *See* Neil v. Nesbit, No. 13-cv-03809, 2014 WL 4897315, at *2 (N.D. Ill. Sept. 27, 2014) (disclosure to plaintiff's co-workers and employers constitutes a class to which the special relationship exception applies satisfying the publicity requirement of the false light tort); Poulos v. Lutheran Soc. Servs. of Illinois, Inc., 728 N.E.2d 547, 556 n.1 (Ill. App. Ct. 2000) ("The reasoning in *Miller* is sound. That reasoning is also persuasive with regards to actions for false light. It is therefore adopted."). After the court in *Poulos* applied the special relationship rule to false light cases, several other courts considering false light cases found the rule instructive. *See* Kurczaba v. Pollock, 742 N.E.2d 425, 437 (Ill. App. Ct. 2000) (holding the publicity requirement satisfied when false information about a Polish immigration attorney was shared with prominent members of the Polish community).

254. *See generally* KREBS & DUNCAN, *supra* note 41.

255. *See generally* RESTATEMENT (SECOND) OF TORTS § 652E (AM. LAW INST. 1977).

256. *See id.*

The difficulty in asserting this cause of action will be showing that the information was widely disseminated or subject to a special relationship and that the information is "highly offensive to a reasonable person."[257] The court will apply the objective test based on the sensitivity of an individual with "ordinary sensibilities."[258] Because medical information is inherently private in nature,[259] any disclosure of medical information would likely be considered objectively offensive by a reasonable person. Further, because the medical information collected by these medical apps paints a skewed picture of the individual, often including many irrelevant details (such as location near a fast food restaurant), the disclosure of the information is likely to be a misrepresentation of the individual's health. However, the false light claim does not help someone whose medical information is disclosed in a way that is an accurate reflection of the person, even though such information could lead to discrimination against the person and even though that is the very type of information that is protected under HIPAA when it is in the records of health care providers.

4. Unjust Enrichment

When app developers and data aggregators profit from a user's information collected from medical apps and do not share their profits with the user, this could give rise to a claim for unjust enrichment. Unjust enrichment occurs when a "person who is unjustly enriched at the expense of another is subject to liability in restitution."[260] Generally, unjust enrichment requires: (1) that the defendant unjustly retained a benefit; (2) that benefit was to the disadvantage of the plaintiff; and (3) the defendant's continued retention of said benefit would violate justice, equity, and good conscience.[261] An unjust enrichment cause of action "does not require fault or illegality on the part of [the] defendant" but is based on the fact that "one party is enriched and it would be unjust for that party to retain the enrichment."[262] Unjust enrichment claims have traditionally been

257. *See id.* § 652D, cmt. c.

258. *See* Pierson v. News Group Publ'ns, Inc., 549 F. Supp. 635, 641 (S.D. Ga. 1982).

259. *See* Miller v. Motorola, Inc., 560 N.E.2d 900, 903 (Ill. App. Ct. 1990).

260. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 (AM. LAW INST. 2011).

261. *See* HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc., 545 N.E.2d 672, 679 (Ill. 1989) (citing Drury v. County of McLean, 433 N.E.2d 666, 669–70 (Ill. 1982)); Kenneke v. First National Bank, 382 N.E.2d 309, 310 (Ill. App. Ct. 1978)).

262. *See* Fortech, L.L.C. v. R.W. Dunteman Co., 852 N.E.2d 451, 463 (Ill. App. Ct. 2006) (quoting Stathis v. Geldermann, Inc., 295 Ill. App.3d 844, 864 (1998)).

used to cover gaps left by statutory legal categories like contract, tort, and property law.[263]

Unjust enrichment has been described as providing "new solutions to old problems."[264] But the opposite is also true: unjust enrichment claims are old solutions that can address new problems. For example, when patients funded a doctor's research program and contributed their tissue for his research and he patented their genetic information without their consent, a court held that the patients had stated a cause of action for unjust enrichment.[265]

In the instance where an app is providing free content or a free service in exchange for marketing the user's information, courts might be reluctant to find unjust enrichment. However, plaintiffs could argue that it was unjust to not inform them about the disclosure practices and that they would have chosen a different app had they known that their information would be marketed to third parties. Judicial outcomes where plaintiffs employed this strategy have varied. In *In re Target Corp. Data Sec. Breach Litigation*,[266] a Minnesota District Court held that the plaintiff's assertion met the requisite requirement for a Minnesota unjust enrichment claim that the defendant "knowingly received or obtained something of value . . . which [it] 'in equity and good conscience' should not have received."[267] In contrast, in the 2016 case *Carlsen v. GameStop, Inc.*,[268] the Eighth Circuit rejected the plaintiff's assertion that he would not have done business with GameStop had he known of its actual privacy practices.[269] The court held that the plaintiff failed to state a claim for unjust enrichment because he did not establish actual injury.[270]

In the case of *In re Nickelodeon*,[271] the federal district court in New Jersey rejected an unjust enrichment claim against Nickelodeon for its data mining practices, stating that "it does not follow that personal information of the type collected by Viacom and Google has actual monetary value to Plaintiffs themselves."[272] But this is

---

263. *See* David N. Fagan, *Achieving Restitution: The Potential Unjust Enrichment Claims of Indigenous Peoples Against Multinational Corporations*, 76 N.Y.U. L. REV. 626, 629 (2001); Candace Saari Kovacic-Fleischer, *Restitution in Public Concern Cases*, 36 LOY. L.A. L. REV. 901, 904 (2003) (noting that this trend is especially true due to the nature of the common law system).

264. *See* Fagan, *supra* note 261, at 629 n.11.

265. *See* Greenberg v. Miami Children's Hosp. Research Inst., Inc., 264 F. Supp. 2d 1064, 1065–66 (S.D. Fla. 2003).

266. 66 F. Supp. 3d 1154 (D. Minn. 2014).

267. *See id.* at 1177 (citing ServiceMaster of St. Cloud v. GAB Bus. Servs., Inc., 544 N.W.2d 302, 306 (Minn. 1996)).

268. 833 F.3d 903 (8th Cir. 2016).

269. *Id.* at 907.

270. *Id.* at 912.

271. No. 12–07829, 2014 WL 3012873 (D. N.J. July 2, 2014).

272. *Id.* at *3. A similar case in California held that the plaintiffs had failed to allege unjust enrichment against a data aggregator for harvesting their data,

erroneous since individual pieces of data do have monetary value to the app user;[273] the app DataWallet even lets users sell their information to marketers.[274] The app Paribus tracks the user's online purchases, keeping user data in exchange for saving the user money on her purchases.[275] In a recent case in a federal district court in Michigan, the court ruled that the plaintiffs had sufficiently pled an unjust enrichment claim because, by selling the plaintiffs' personal reading information, the defendants made the plaintiffs' subscriptions less valuable since companies would already know their reading habits, and the defendants made a profit from selling these data.[276]

An unjust enrichment claim also requires that the retention of the benefit would violate justice, equity, and good conscience.[277] The strongest argument for this is that health-related information is treated as private in our society.[278] Allowing app developers to sell such private information and retain the benefit violates entrenched notions of justice.

If the app user consented to the disclosures, she cannot state a claim for unjust enrichment.[279] The Tenth Circuit has explained that consent exists if (1) there is a visible notice of accompanying terms and (2) there is an indication on the part of the user that the terms were accepted.[280] If these two conditions are not met, the privacy policy and terms and conditions most likely do not form an enforceable contract. In *Hines v. Overstock.com, Inc.*,[281] the Eastern District of New York court determined that because the Terms and Conditions were "not prominently displayed so as to provide

---

because the plaintiffs had not sustained an economic injury in fact needed to establish Article III standing. *See* LaCourt v. Specific Media, Inc., No. SACV 10–1256–GW (JCGx), 2011 WL 1661532, at *3, *5 (C.D. Cal. Apr. 28, 2011).

273. *See* Alexis C. Madrigal, *How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $1,200*, THE ATLANTIC (Mar. 19, 2012), https://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730/.

274. *See* Melia Robinson, *This App Lets You Make Easy Money by Selling Personal Data to Marketers*, BUS. INSIDER (June 10, 2016), http://www.businessinsider.com/datawallet-lets-you-sell-your-data-2016-6.

275. PARIBUS, https://paribus.co/ (last visited Aug. 10, 2018).

276. *See* Moeller v. Am. Media, Inc., 235 F. Supp. 3d 868, 876 (E.D. Mich. 2017).

277. HPI Health Care Serv., Inc. v. Mt. Vernon Hosp., Inc., 545 N.E.2d 672, 679 (Ill. 1989).

278. *See* Sheila A.M. McLean, *International Commentaries Genetic Screening of Children: The U.K. Position*, 12 J. CONTEMP. HEALTH L. & POL'Y 113, 117 (1995).

279. *See* Hancock v. Am. Tel. & Tel. Co., Inc., 701 F.3d 1248, 1256–57 (10th Cir. 2012) (examining a user's consent to terms and conditions and the validity of that contract); First Midwest Bank v. Cobo, 90 N.E.3d 567, 575 (Ill. App. 2017) (stating that a party cannot state a claim for unjust enrichment where an express contract exists between the parties and concerns the same subject matter).

280. *See Hancock*, 701 F.3d at 1256–57.

281. 668 F. Supp. 2d 362 (E.D. N.Y. 2009).

reasonable notice of the Terms and Conditions" and the website "did not prompt [the user] to review the Terms and Conditions," a contract did not exist.[282] As noted in *Nguyen v. Barnes & Noble Inc.*,[283] when the user has no actual notice of the Terms and Conditions or privacy policy, the validity of the contract depends on the prominence of the agreement on the website.[284] In *Nguyen*, the Ninth Circuit ruled that without notice or prompts to the user, the location of a hyperlink to the terms on the website provided insufficient notice and therefore did not constitute a contract.[285] Similar to having an ambiguous term in the contract, the Ninth Circuit argued that while a "failure to read" does not relieve a party from the contract,[286] "the onus must be on website owners to put users on notice of the terms to which they wish to bind consumers."[287]

Unjust enrichment claims may work in some cases involving the disclosure of information from medical apps, particularly if the aggregation and sale of the user's data was not disclosed in advance. For example, in our study of medical mobile apps, only 19% of diabetes apps and only 38% of psychiatric apps had a privacy policy.[288] In cases where the plaintiff was not informed of the developer's practices, an unjust enrichment claim could potentially apply. But there are substantial hurdles. It may be difficult to show that the app developer has *unjustly* been enriched, particularly since data aggregation is viewed as a legitimate business enterprise.[289] It is almost impossible to claim unjust enrichment if the app developer disclosed its practices in a privacy statement and the consumer nonetheless used the app.[290] It will also be difficult to prove that the user was "disadvantaged" because, even if the disclosed information was the basis for an adverse decision against the individual, she may never learn that the data disclosed was used to her disadvantage.

IV. ALTERNATIVES TO EXISTING LEGAL POLICIES

People care deeply about the privacy of the information collected by their medical apps.[291] Yet our studies show that information from

282. *Id.* at 367.

283. 763 F.3d 1171 (9th Cir. 2014).

284. *See id.* at 1176–77.

285. *Id.* at 1178–79.

286. *Id.* at 1179 (citing Gillman v. Chase Manhattan Bank, N.A., 534 N.E.2d 824, 829 (N.Y. 1988)).

287. *Id.*

288. *See infra* Table 1.

289. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001).

290. *See In Re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 982 (S.D. Cal. 2014) (accepting disclaimers in Sony's privacy policy by registering for and using Sony's online interactive network).

291. After Edward Snowden released documents about NSA surveillance, Pew conducted a survey about what data individuals considered to be sensitive information. 81% of respondents considered health information as sensitive data

medical apps is collected directly and indirectly and then shared with marketers and other third parties in ways which can harm the app user. Vast in scope and packaged with information not traditionally thought of as implicating health, information from medical apps is sold to third parties including employers and insurers.[292] In one instance, an insurer bought health-related digital data from about three million people from a data aggregator.[293]

Existing laws do not sufficiently protect the privacy of medical app users. An alternative approach is necessary that recognizes the unique challenges raised by medical apps in terms of the scope of information they collect, the nature of that information, and the context in which it is collected. Merely extending existing protections for health information to the app context falls short. Apps collect information, such as gait, GPS location, purchase of unscented lotion, and so forth, that can be indicative of health but is not considered

(55% considered health information "very sensitive" and 26% considered health information "somewhat sensitive"). Among 16 different types of data, health information was considered the second most sensitive type of data, following one's social security number. *See* MARY MADDEN ET AL., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 32 (2014), www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf. An October 2014 Symantec survey also found that of 662 U.S. smartphone users, less than one-fifth of respondents (18%) reported that they would be willing to allow access to their fitness or health information to use an app for free. *See Norton Mobile Apps Survey Report*, SYMANTEC (Dec. 10, 2014), https://www.slideshare.net/symantec/norton-mobile-apps-survey-report. The June 2015 Healthline survey of 3,679 readers also found that a quarter of respondents reported concerns about the security of their personal health information on health tracking apps like Fitbit and 45% of respondents reported concerns about their wearables being hacked to steal their personal health information. *See* David Mills, *Consumers Like Wearable Technology But Worry About Data Security*, HEALTHLINE (July 28, 2015), http://www.healthline.com/health-news/consumers-concerned-about-privacy-personal-health-data-wearables-mobile-apps-072815#1. The authors of a study of the twenty most popular health and fitness apps suggest that as these privacy practices, or lack thereof, come to light, there may be an increased user demand for health and fitness apps that are more transparent about their use of consumer data. *See* Rowan & Dehlinger, *supra* note 97, at 354.

292. *See* Michael Fertik, *Your Future Employer Is Watching You Online. You Should Be, Too*, HARV. BUS. REV. (Apr. 3, 2012), https://hbr.org/2012/04/your-future-employer-is-watchi (noting that employers undertake online research about job applicants); Bernard Marr, *How Big Data Is Changing Insurance Forever*, FORBES (Dec. 16, 2015), https://www.forbes.com/sites/bernardmarr/2015/12/16/how-big-data-is-changing-the-insurance-industry-forever/#65fcc588289b (noting that insurance companies use big data to set insurance premiums).

293. *See* Beckett, *supra* note 57; Jen Wieczner, *How the Insurer Knows You Just Stocked Up on Ice Cream and Beer*, WALL ST. J. (Feb. 25, 2013), https://www.wsj.com/articles/SB10001424127887323384604578326151014237898.

"health" information under HIPAA.[294] Whatever policy is adopted, it is important not to duplicate the limitations of HIPAA, the federal and state statutes, and some of the state tort precedents in terms of what information is covered.

A new privacy paradigm is necessary. I have come to that conclusion based on an exploration of the two existing models that have been traditionally used to protect health-related information. The first relies on advance notice to the user about privacy policies and the solicitation of consent. This is the approach used by HIPAA.[295] The second is to completely ban the collection and disclosure of medical information. This is the approach taken in the employment situation where, under various laws,[296] an employer cannot ask a job applicant about medical conditions, even if the applicant would have been willing to give that information. Similarly, the Genetic Information Nondiscrimination Act[297] prohibits insurers and employers from asking individuals about their genetic information. Additionally, various legal concepts from fiduciary duty to warranty prohibit doctors from using a person's health information in ways that could harm that person.[298]

A. The Notice Model

Recent efforts to protect the privacy of medical app information, such as the statutes adopted in California and Texas,[299] incorporate the notice model of HIPAA through a requirement that the medical app developer notify the user in advance about its data collection and dissemination practices. The notice model falls short for a variety of reasons. One problem with the notice model is that it embodies a take-it-or-leave-it approach, where a user has to forego the app altogether or agree to "pay" for the app (instead of or in addition to a purchase price) by allowing the app developer to market the user's information. If the user is dependent on an app to manage her

294. For example, Blue Chip Marketing found patients for an obesity drug by targeting people who subscribe to premium cable and frequent fast food dining, characteristics that suggest a sedentary lifestyle. *See* Walker, *supra* note 57.

295. *See* Notice of Privacy Practices For Protected Health Information, 45 C.F.R. § 164.520 (2018).

296. *See, e.g.*, Americans with Disabilities Act, 42 U.S.C. §§ 12111–12117 (2012).

297. *See* Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. §§ 300gg-53, 1320d-9, 2000ff, 200ff-1–2000ff-11 (2012).

298. *See* ANDREWS, *supra* note 38.

299. *See* CAL. CIV. CODE § 56.06 (West 2018); TEX. HEALTH & SAFETY CODE ANN. § 181 (West 2018).

condition, or is required by her physician,[300] employer,[301] or Medicaid[302] to use an app, she has no choice but to give up her privacy.

The notice model also fails because the privacy policies are routinely difficult to find, hard to understand, and too numerous to read. Users rarely read app privacy policies,[303] at times because they think that the mere existence of a privacy policy means that their personal information is protected.[304] But 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 did those without privacy policies.[305] Even when users do read privacy policies, they often do not understand them or their implications.[306] Privacy policies of health and fitness apps generally are too long and incomprehensible for the average user to meaningfully read and understand.[307] Even app developers themselves admit to difficulties

300. Seven percent of physicians prescribe apps. *See* Bauer et al., *supra* note 46.

301. *See* Grant, *supra* note 49. For example, CoreHealth offers apps designed for workplace wellness programs. *See* COREHEALTH TECH., https://corehealth.global/wellnessplatform (last visited Aug. 10, 2018).

302. 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 voluntary, Medicaid benefits could be conditioned on medical app use in the future.

303. According to a 2012 study, only 16% of people claim to read privacy policies of the services they use. *See* INTERNET SOC'Y, GLOBAL INTERNET USER SURVEY SUMMARY REPORT 1, 4 (2012), http://wayback.archive-it.org/9367/20170907075228/https://www.internetsociety.org/sites/default/files/rep-GIUS2012global-201211-en.pdf.

304. Many people do not attempt to read privacy policies under the mistaken assumption that simply the existence of a privacy policy indicates that their data cannot be shared with others without their permission. *See* JOSEPH TUROW ET AL., THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 8 (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf. Another study found that many respondents (65%) did not know that the statement, "When a website has a privacy policy, it means the site will not share my information with other websites and companies without my permission," is false. *See id.*

305. 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., *supra* note 102.

306. *See* CHIN ET AL., *supra* note 148, at 11; FELT ET AL., *supra* note 89; *A Conundrum of Permissions: Installing Applications on an Android Smartphone*, *supra* note 89, at 70.

307. *See* Rowan & Dehlinger, *supra* note 97, at 353–54.

in reading privacy policies,[308] but this should come as no surprise considering the average reading grade level of health app privacy policies is above the 12th grade level,[309] and privacy policies are often intentionally bewildering.[310]

Relying on advance notice through privacy policies is not sufficiently protective because, 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 that a modern individual comes in contact with to assure that she is aware of her rights and is able to safeguard them. Most people just click "okay."[311] We can hold people to their legal choices based on notices in certain contracts—such as one for buying a house—because of the uniqueness and economic impact of a house purchase, which makes it more likely that the reader will pay attention to the terms of the house contract.[312] But 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.[313] A Carnegie Mellon study has shown that it would take a person thirty days to read the privacy statements of the apps and websites that she commonly uses.[314]

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 "privacy policies," some policies say they give rise to no rights,[315] while others

---

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

309. *See* Rowan & Dehlinger, *supra* note 97, at 352.

310. *See* Pollach, *supra* note 97, at 107.

311. 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 3 (2014), http://worldcomp-proceedings.com/proc/p2014/SAM9775.pdf.

312. *See* Schnabel v. Trilegiant Corp., 697 F.3d 110, 120 (2d Cir. 2012).

313. *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.

314. *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).

315. *See Privacy Policy*, WHATSMYM3, https://www.whatsmym3.com /PrivacyPolicy.aspx (last visited Aug. 10, 2018) ("This Privacy Policy is not intended to and does not create any contractual or other legal rights on behalf of any party.").

say that they can change their terms at any time.[316] 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.

B. A Ban on Disclosure of Information from Medical Apps

An alternative approach is necessary that recognizes the unique challenges raised by medical apps in terms of the scope, nature, and context of the information they collect. To truly protect health privacy, a new policy must be adopted to protect all the information collected by health apps. We need to go back to the basics and recognize that protecting medical app information serves the same purposes as protecting information in the hands of physicians or health care institutions. Such protection encourages people to use a service that can help them prevent, manage, and treat diseases and disorders. It can also protect them from discrimination based on their health status or their interest in learning more about their health.

The need for such protections has led me to this controversial proposal: medical apps should not share any information with data aggregators, marketers, or other third parties besides (at the user's explicit request) the user's designated health care providers. This is in keeping with how society protects health information collected by doctors. Law, ethics, and social norms do not allow doctors to sell that information to marketing companies. Physicians must keep the entire patient record private, even information that is about a patient's lifestyle, relationships, work, or other facts that are not necessarily thought of as health information.[317]

This protection of privacy of information by banning particular practices in the collection and dissemination of health-related information is not without precedent. Under the Americans with Disabilities Act, potential employers are prohibited from obtaining medical information about applicants before offering employment.[318] The policies behind that approach include furtherance of human dignity, protecting an applicant against discrimination, and recognizing that absent a ban a potential employer might surreptitiously use the information to discriminate, and the potential employee might not realize that health information was the basis for

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

317. *See* Uses and Disclosures for Which an Authorization is Required, 45 C.F.R. § 164.508 (2018).

318. *See* Americans with Disabilities Act, 42 U.S.C. §§ 12111–12117 (2012).

the unfair discrimination.[319] These rationales similarly support the ban on the dissemination of information from medical apps since such a ban can protect a person's dignity and prevent discrimination against a person in obtaining a job, a credit card, life insurance, a date, nursing home admission, and other benefits and necessities. A ban on dissemination of medical app information is particularly important because app developers, unlike doctors, have no fiduciary duty to act in the best interests of their users.[320]

Opponents of what I am proposing may argue that my approach will reduce the availability of medical apps since developers can fund the cost of creating a medical app through money raised by selling the individual's private information to third parties. I do not consider potential shrinkage in the medical app market, as it is currently constituted, to be problematic. Some medical apps do not provide much benefit to their users, while at the same time they surreptitiously collect information that could harm the user greatly. This is the case with the diabetes app[321] which merely provided a dozen recipes yet could turn on the phone's microphone to collect intimate information about the user, even though the microphone had no role in the user's access to recipes.

With the incentive of being able to garner huge amounts of money by selling private data from medical apps, unscrupulous individuals have entered the market as developers and unsafe apps have entered users' hands. Because medical apps provide the important functions of diagnosing and recommending treatment for disease, the results can be deadly. Many people use medical apps to take the place of a doctor.[322] In the ISLAT studies, 43% of diabetes apps were designed for disease management and 19% allowed the user to calculate insulin doses and the amount of carbohydrates consumed. Thirty-five percent of the bipolar apps we examined in the ISLAT study similarly tracked medications, vitals, or symptoms. Forty-one percent told the user what dose of a drug to take or what other action the user should

319. *See generally* Editorial Board, *Protecting Employees' Health Data*, N.Y. TIMES (Mar. 26, 2016) https://www.nytimes.com/2016/03/27/opinion/sunday/protecting-employees-health-data.html (discussing issues with employers having access to health information beyond just disabilities).

320. *See generally* Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ (discussing how websites and technology providers are similar to doctors and others with fiduciary relationships, but do not have similar duties).

321. *See supra* text accompanying notes 120–22.

322. *See* Soumya Karlamangla, *Health Apps: Unlimited Promise or 'Like Having a Really Bad Doctor'*, L.A. TIMES (Apr. 12, 2016), http://www.latimes.com/business/technology/la-me-mobile-health-safety-20160412-story.html.

undertake to treat her condition.[323] But often the advice given by medical apps and the treatment recommendations are wrong.[324]

In our study, we found apps that offered unproven treatments. Several apps aimed at treating bipolar disorder actually discouraged going to the doctor or taking recommended medications, and instead advertised to users that they provided "Doctor's #1 recommendation for mental illness treatment"—soothing sounds.[325] When we tested apps that were supposed to warn about drug interactions, 67% failed to recognize a potentially fatal interaction.[326] None of the medication tracking apps gave a warning when we input a lethal 6000 mg. dose of lithium.[327] In fact, one of the apps even brought up an advertisement offering to sell us more lithium at a discounted price.[328] Other studies have shown deficiencies in asthma apps,[329] diabetes apps,[330] and other medical apps.[331]

In rare and egregious instances, the FTC has stepped in—for example, when an app falsely purported to cure acne through blue

---

323. *See also* Stephanie Baum, *Merck KGaA Adopts Medisafe Medication Adherence Tool for Patients with Chronic Conditions*, MEDCITYNEWS (Mar. 27 2018), https://medcitynews.com/2018/03/merck-kgaa-adopts-medisafe-medication-adherence-tool-patients-chronic-conditions/.

324. *See infra* text accompanying notes 325–31.

325. *See Ocean Sleeper Sound*, APTOIDE, https://ocean-sleeper-sound.en.aptoide.com/ (last visited Aug. 10, 2018).

326. The drug interactions that could potentially result in death, among other side-effects, were lithium and arsenic trioxide, and Prozac and lithium for "CareZone," since "CareZone" did not recognize arsenic trioxide. For the interaction between lithium and arsenic trioxide, see *Drug Interaction Report*, DRUGS.COM, https://www.drugs.com/interactions-check.php?drug_list=236-0,1477-0 (last visited Aug. 10, 2018). For the interaction between Prozac and lithium, see *Drug Interactions Between Lithium and Prozac*, DRUGS.COM, https://www.drugs.com/drug-interactions/lithium-with-prozac-1477-0-1115-648.html (last visited Aug. 10, 2018). Four of six apps did not notify the user of a problem. *See* CAREZONE, https://carezone.com/home (last visited Aug. 10, 2018); *DBSA Wellness Tracker*, DEPRESSION AND BIPOLAR SUPPORT ALLIANCE, https://secure2.convio.net/dabsa/site/SPageServer/?NONCE_TOKEN=ABC0F1FFE6C38CED122884DE3905B986&pagename=wellness_tracker (last visited Aug. 10, 2018); MEDHELPER APP, http://medhelperapp.com/ (last visited Aug. 10, 2018); MEDISAFE, https://medisafe.com/ (last visited Aug. 10, 2018).

327. This chart of statistics on drug overdoses notes that the minimum lethal dosage for lithium is fifteen 300 mg. pills, or 4500 mg. total. *See Drug MLDs*, LOST ALL HOPE, http://lostallhope.com/suicide-methods/drug-poisoning/drug-mlds (last visited Aug. 10, 2018).

328. *See* MEDISAFE, *supra* note 326.

329. *See* Kit Huckvale et al., *Apps for Asthma Self-Management: A Systematic Assessment of Content and Tools*, 10 BMC MED. 1, 8–9 (2012).

330. *See Class 2 Device Recall ACCUCHEK Connect Diabetes Management App*, FOOD & DRUG ADMIN., https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?id=134687 (last updated Aug. 9, 2018).

331. *See* Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief at 7–8, Fed. Trade Comm'n v. Lumos Labs, Inc., No. 3:16-cv-00001. (N.D. Cal. Jan. 8 2016), https://www.ftc.gov/system/files/documents/cases/160105lumoslabsstip.pdf.

light from the app[332] or when a mole app purported to be able to diagnose a lesion as skin cancer by comparing it to photos of other lesions.[333] Because medical apps are not vetted in advance by the Food and Drug Administration unless they are part of an already-regulated device, such as an insulin pump,[334] many dangerous apps have entered the market.

By taking away the incentive of data marketing, shoddy app makers who care more about collecting information than addressing a medical need will be driven from the market. The cost of medical apps might increase, but there will be a role for disease organizations to fund development of apps and to fund physician-patient validation of apps. With fewer apps, the Food and Drug Administration might be able to exert greater oversight, and health care entities will be able to serve more readily as curators of apps, providing guidance to consumers. Under the current system, medical app users are not only giving up their privacy, but also risking their health.

V. CONCLUSION

Tens of thousands of medical apps are currently available to help people diagnose, manage, treat, and prevent diseases from A (asthma) to Z (zinc deficiency). However, those apps are poorly regulated and create hazards to people's health and their privacy. In our novel studies of medical apps related to diabetes, bipolar disorder, suicide, and eating disorders, we found that information from medical apps is collected directly and indirectly and then shared with marketers and other third parties in ways which can harm the app user. Current laws do not adequately protect medical app users. A preferable approach would be to forbid altogether the disclosure of information collected by medical apps to marketers, data aggregators, and other third parties.

---

332. *See* Press Release, Fed. Trade Comm'n, 'Acne Cure' Mobile App Marketers Will Drop Baseless Claims Under FTC Settlements (Sept. 8, 2011), http://www.ftc.gov/news-events/press-releases/2011/09/acne-cure-mobile-app-marketers-will-drop-baseless-claims-under.

333. Two other apps, "MelApp" and "Mole Detective," both claimed to diagnose melanomas even in the earliest stages. Both apps had the user take a picture of their mole and input information about it, and the app would classify the mole's melanoma risk on a scale from low to high. But according to the FTC, there was no scientific proof. The claims were not supported, and the FTC forced a settlement with both companies over the false claims. *See* Karra, *supra* note 12.

334. *See* FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 14–15 (2015), http://www.fda.gov/downloads/MedicalDevices/. . ./UCM263366.pdf.

APPENDIX: TABLES

TABLE 1: AVAILABILITY AND ACCESSIBILITY OF MEDICAL APP PRIVACY POLICIES

	% of Apps with Privacy Policies	**% of Privacy Policies Linked from the Description of the App on Google Play**	**% Only on Developers' Websites**	**% Difficult to Tell Whether Privacy Policy Applied to the App**
Diabetes Apps	19% (41 of 211)	80% (33 of 41)	20% (8 of 41)	0% (0 of 41)
Bipolar Apps	41% (26 of 63)	73% (19 of 26)	27% (7 of 26)	23% (6 of 26)
Eating Disorder Apps	36% (12 of 33)	50% (6 of 12)	50% (6 of 12)	33% (4 of 12)
Suicide Prevention Apps	34% (11 of 32)	82% (9 of 11)	18% (2 of 11)	45% (5 of 11)
Psychiatric Apps (Combined)	38% (49 of 128)	69% (34 of 49)	31% (15 of 49)	31% (15 of 49)

TABLE 2: PRIVACY POLICY PROVISIONS FOR INFORMATION COLLECTION FROM PRIVACY POLICIES AVAILABLE PRE-DOWNLOAD AND APPLICABLE TO THE APP

Type of Privacy Policy Provision	**Diabetes Apps (n=41) (%)**	**Bipolar Apps (n=22) (%)**	**Eating Disorder Apps (n=8) (%)**	**Suicide Prevention Apps (n=6) (%)**	**Psychiatric Apps (Combined; n=36) (%)**
Personal Information					
Collected when app is used	51	82	100	67	61
Stored in the developer's system	44	68	63	67	49
Location Tracking (approximate cell tower and/or precise GPS location)	Not Analyzed	45	25	33	29
Log files will be collected	17	73	50	50	47
IP address will be collected	N/A	68	50	67	47
Encrypts user data	54	50	0	17	24
Means of Collection					
Cookies will be used	49	86	75	33	55
Web beacons will be used	N/A	36	25	50	27
Tracking mechanisms (cookies, web beacons, or both) used	49	91	75	50	59

User Options					
Can opt out of cookies	32	59	13	17	42
Can opt out of web beacons	N/A	0	0	0	0
Can opt out of receiving emails	22	50	25	0	27
Can opt out of receiving marketing materials	15	46	25	0	24

TABLE 3: PRIVACY POLICY PROVISIONS FOR INFORMATION DISSEMINATION

Type of Privacy Policy Provision	**Diabetes Apps (n=41) (%)**	**Bipolar Apps (n=22) (%)**	**Eating Disorder Apps (n=8) (%)**	**Suicide Prevention Apps (n=6) (%)**	**Psychiatric Apps (Combined, n=36) (%)**
Shared with advertisers	7	5	0	0	3
Shared if required by law	61	82	50	67	53
Shared in the event of a merger or acquisition	24	50	38	33	33
Not sold	22	41	13	17	22
Only disclosed with user's consent	29	36	0	0	22
May be transferred to various countries around the world	27	41	13	50	27
May be used for advertisement	39	5	13	0	6

TABLE 4: PERMISSIONS FOR MOBILE HEALTH APPS

Permission	Diabetes Apps (n=211) (%)	Bipolar Apps (n=63) (%)	Eating Disorder Apps (n=33) (%)	Suicide Prevention Apps (n=32) (%)	Psychiatric Apps (Combined; n=128) (%)
Find accounts on the device	14	25	12	38	25
Read your contacts	6	8	6	19	10
Approximate location (network-based)	12	16	21	28	20
Precise location (GPS and network-based)	15	17	30	31	24
Either approximate or precise location	18	21	30	31	26
Directly call phone numbers	6	5	6	22	9
Read phone status and identity	31	32	30	31	31
Modify or delete the contents of your USB storage	64	62	58	31	53
Read the contents of your USB storage	1	62	58	34	54
Take pictures and videos	11	13	30	13	17
View Wi-Fi connections	12	22	24	34	26

Record audio	4	5	3	13	6
Full network access	83	94	91	91	92
Use accounts on the device	2	5	3	6	5
View network connections	63	86	91	78	85
Receive text messages (SMS)	2	3	0	6	3
Reroute outgoing calls	0	0	0	3	1
Read your Web bookmarks and history	1	2	0	0	1
Draw over other apps	1	5	0	3	3
Google Play license check	5	2	3	0	2
Write web bookmarks and history	0	2	3	0	2

TABLE 5: GPS PERMISSION ACCESS AND THE EXISTENCE OF PRIVACY POLICIES

	Number of Apps with Access to Location	**% of Apps with Access to Location without Privacy Policies**	**% of Apps with Access to Location and Privacy Policies that Do Not Mention Location**
Diabetes Apps	37	65% (24 of 37)	Not Analyzed
Bipolar Apps	13	54% (7 of 13)	15% (2 of 13)
Eating Disorder Apps	10	40% (4 of 10)	30% (3 of 10)
Suicide Prevention Apps	10	50% (5 of 10)	10% (1 of 10)

TABLE 6: ACCESS AND TRANSMISSION PRACTICES OF DIABETES AND BIPOLAR APPS

	Diabetes Apps (n=65) (%)	**Bipolar Apps (n=26) (%)**
Share information with advertising networks or data analytics companies	77	69
Send related ads	11	12
Collect medication information	34	27
Collect sleep information	Not Analyzed	42
Collect exercise information	17	27
Access photos	58	19
Access media	52	8
Access files	66	54
Full network access	100	27
Receive data from Internet	100	96
Access Device ID	98	38
View network connections	63	88
Access contacts	6	23
Access phone number or phone calls	11	15
Send text messages	15	0
Access camera	9	12
Access microphone	6	4
Access Wi-Fi connection information	29	38
Access geolocation	29	19
Sent transmissions to DoubleClick	25	50
Sent transmissions to Google Analytics	31	42

TABLE 7: STUDIES OF MOBILE MEDICAL APPS AND ENCRYPTION OF DATA

Study	**% of Apps that Encrypted Transmissions**
ISLAT Diabetes App Study	100% (65 of 65)
ISLAT Bipolar App Study	42% (11 of 26)
Privacy Rights Clearinghouse Study[335]	12% (5 of 43)
Knorr et al. Blood Pressure & Diabetes App Study[336]	1% (1 of 72)
Study	**% of Apps that Encrypt Data Stored on the Phone**
ISLAT Diabetes App Study	2% (1 of 65)
Privacy Rights Clearinghouse Study[337]	0% (0 of 43)

335. Ackerman, *supra* note 81, at 5.
336. Knorr et al., *supra* note 83, at 579.
337. Ackerman, *supra* note 81, at 20.

***