Richmond Journal of Law & Technology Volume XXVIII, Issue 1

RESPONDING TO THE DIGITAL HEALTH REVOLUTION

James Stramm*

Cite as: James Stramm, *Responding to the Digital Health Revolution*, 28 RICH. J.L. & TECH., no. 1, (2021).

* Law Clerk. J.D., Harvard Law School, 2021. Thank you to Terry Fisher and Yochai Benkler for their comments, and to Martha Minow for her constant support and guidance.

ABSTRACT

This Article describes how dominant technology firms have revolutionized the healthcare industry in only a few years. Now, medical treatment and research are predicated on constant, decentralized data collection, prediction and personalization, and algorithmic judgments. The new digital health paradigm implicates issues of privacy, bias, autonomy, equity, and discrimination. Yet Big Tech has been quick to justify its new practices as an opportunity for better care, quicker discovery of cures, and ultimately, lives saved. Moreover, many medical practitioners welcome this healthcare revolution as a chance to deemphasize the importance of patient privacy and autonomy in American bioethics and prioritize the free flow of medical information to improve health systems. Whatever the merits of the new regime, current legislation is ill-suited for a data-driven approach to healthcare because it leaves gaps in regulation and harms unaddressed.

This Article argues that while reform is necessary, new regulation should not reflexively guard patient privacy. Rather, any legislative response must also account for other concerns like bias, equity, autonomy, and collective benefit. These considerations are often at odds with one another, and tradeoffs are unavoidable. This Article offers a framework for evaluating new digital healthcare tools in the context of these conflicting fundamental values, accounting for harms and benefits at both the individual and societal level. Finally, this Article suggests a number of legislative requirements necessary for any regulation to adequately respond to the digital health revolution.

"If you zoom out into the future, and you look back, and you ask the question, 'What was Apple's greatest contribution to mankind?' It will be about health." – Tim Cook[1]

I. INTRODUCTION

[1] Dominant technology firms have disrupted and revolutionized virtually every sector of the economy. In each industry, these "Big Tech" firms have presented users with a now-familiar bargain: give us your personal data in exchange for services and insights based on algorithmic prediction and personalization.[2] Recently, tech titans have turned their sights to the healthcare industries to collect "perhaps the last bounty of personal data yet to be scooped up."[3] In medical contexts, the "Big Data bargain" comes with higher stakes—personal health data is often the most sensitive and closely-guarded information, heightening issues like autonomy and privacy; indeed, inaccurate or biased algorithmic healthcare decisions can have life-or-death consequences.[4] But along with the healthcare bargain comes the chance for more significant payoffs by stimulating research, improving treatment and care, better informing healthcare-related policy, and ultimately, saving lives.

[1] Lizzy Gurdus, *Tim Cook: Apple's Greatest Contribution Will Be 'About Health'*, CNBC (Aug. 9, 2019, 10:52 AM), https://www.cnbc.com/2019/01/08/tim-cook-teases-new-apple-services-tied-to-health-care.html [https://perma.cc/DNJ8-E574].

[2] W. Nicholson Price II & I. Glenn Cohen, *Privacy in the Age of Medical Big Data*, 25 NATURE MED. 37, 41 (2019) ("As an ethical matter data collection is best justified as a kind of 'bargain' struck between data sources and data users — provide us your data, recognizing this may encroach in some ways on your privacy, because it will permit us to provide advances . . . that will improve your life.").

[3] Rob Copeland et al., *Inside Google's Quest for Millions of Medical Records*, WALL ST. J. (Jan. 11, 2020, 12:15 AM), https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700?mod=article_inline [https://perma.cc/5EFX-7S3Y].

[4] *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 681–84 (2016) (providing examples of algorithmic bias and its disparate impact).

[2] Whatever the merits, current data and medical regulatory regimes are unequipped to handle the emerging digital health industry, as they leave privacy harms, algorithmic bias and discrimination unaddressed. While reform is necessary, tradeoffs between competing considerations are unavoidable, as 21st-century insights into data science show that tradeoffs between data harms and benefits are inevitable.[5] This Article offers a framework for evaluating the individual and collective benefits of new digital healthcare tools while accounting for concerns over user privacy, autonomy, dignity, and equity.

[3] Section II details how technology companies vie for user medical data in the new digital health industry. Big Tech's blueprint for healthcare conquest parallels strategies used in other industries, with each development serving the goal of expanding data collection capabilities. Firms design products like smart watches and voice assistants that enable constant tracking of consumers.[6] Titans like Apple and Google acquire health-based tech startups in search of new medical data supply lines.[7] They also work with hospitals and traditional medical providers to develop data-driven machine learning and algorithmic healthcare devices, in exchange for

[5] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010).

[6] *E.g.*, Sarah Mitroff, *Apple Watch Blood Oxygen app: How it works and how to use it*, CNET (Oct. 1, 2020, 10:00 AM), https://www.cnet.com/health/apple-watch-blood-oxygen-app-how-it-works/ [https://perma.cc/P49M-X4HE]; Casey Ross, *New voices at patients' bedsides: Amazon, Google, Microsoft, and Apple*, STAT NEWS (Feb. 6, 2019), https://www.statnews.com/2019/02/06/voice-assistants-at-bedside-patient-care/ [https://perma.cc/3VB6-FYV7].

[7] *E.g.*, Dieter Bohn, *Google is buying Fitbit: now what?*, VERGE (Nov. 1, 2019, 4:15 PM), https://www.theverge.com/2019/11/1/20943993/google-fitbit-acquisition-smartwatch-wearable-fitness-nest-htc-hardware-software [https://perma.cc/3W4R-ADP6]; Christina Farr & Steve Kovach, *Apple bought a start-up that was working on monitoring asthma in children*, CNBC (May 24, 2019, 8:15 PM), https://www.cnbc.com/2019/05/24/apple-acquires-asthma-detection-start-up-tueo-health.html [https://perma.cc/9XC5-N44L]; Nick Statt, *Google just spent $40 million for Fossil's secret smartwatch tech*, VERGE (Jan. 17, 2019, 1:26 PM), https://www.theverge.com/2019/1/17/18187026/google-fossil-group-smartwatch-sale-40-million-wear-os-android [https://perma.cc/CNX4-CNZE].

access to patient health records.[8] Finally, recent developments in data analytics allow companies to infer user medical traits from seemingly non-medical data, turning social media into a treasure trove of healthcare information.[9]

[4] Section III describes the benefits that the new data-driven paradigm offers to individuals, healthcare providers, and researchers, and how Big Tech turns these benefits into corporate gain. For individuals, new health self-tracking devices tap into the zeitgeist of "self-knowledge through numbers."[10] For physicians, new digital health tools promise to reduce burnout by minimizing burdensome tasks like scribing and notetaking.[11] The most significant benefit comes from the potential to save lives through a data-driven approach to research and care. Though potential value exists, tech companies are quick to justify their exploitative tactics under the guise

[8] *E.g.*, Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records*, WALL ST. J. (Jan. 20, 2020, 5:30 AM), https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200 [https://perma.cc/8WT7-8VWJ]; Rob Copeland & Sarah E. Needleman, *Google's 'Project Nightingale' Triggers Federal Inquiry*, WALL ST. J. (Nov. 12, 2019, 11:13 PM), https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867 [https://perma.cc/F8E8-C7PX]; *Microsoft and Providence St. Joseph Health announce strategic alliance to accelerate the future of care delivery*, MICROSOFT NEWS CTR. (July 8, 2019), https://news.microsoft.com/2019/07/08/microsoft-and-providence-st-joseph-health-announce-strategic-alliance-to-accelerate-the-future-of-care-delivery/ [https://perma.cc/4PF4-UWB2].

[9] *See* Mason Marks, *Emergent Medical Data: Health Information Inferred by Artificial Intelligence*, 11 U.C. IRVINE L. REV. 995, 996–97 (2021).

[10] *See* Gary Isaac Wolf, *Quantified Self*, AETHER (Nov. 6, 2009), http://aether.com/quantifiedself [http://web.archive.org/web/20091106094426/http://aether.com/quantifiedself].

[11] Andreea Bodnari, *Healthcare gets more productive with new industry-specific AI tools*, GOOGLE CLOUD: HEALTHCARE & LIFE SCIS. (Nov. 10, 2020), https://cloud.google.com/blog/topics/healthcare-life-sciences/now-in-preview-healthcare-natural-language-api-and-automl-entity-extraction-for-healthcare [https://perma.cc/4L9Y-HF7V].

of saving lives, relying on the familiar self-serving corporate trope of claiming to "make the world a better place."[12]

[5] Section IV documents the potential harms that stem from digital health practices, and the gaps in the regulatory system that leave these harms unaddressed. Many privacy harms already occur in the digital health paradigm, given the decentralized nature of medical data collection and relaxed security practices.[13] Virtually all data security breaches occur beyond the purview of the Health Insurance Portability and Accountability Act (HIPPA),[14] with limited accountability and oversight. Furthermore, algorithmic and machine learning tools already exhibit bias, and are disproportionately more effective for those with better access to healthcare.[15] Even though these harms are already known and understood, tradeoffs between the benefits and harms are unavoidable; individual and collective utility, privacy, autonomy, and equity are often at odds with each other in the digital health paradigm.

[6] Acknowledging the inevitability of these tradeoffs, Section V offers a framework for how to think through competing considerations. Finally,

---

[12] *See* Mat Honan, *Google's Broken Promise: The End of "Don't Be Evil,"* GIZMODO (Jan. 24, 2012, 5:41 PM), https://gizmodo.com/googles-broken-promise-the-end-of-dont-be-evil-5878987 [https://perma.cc/QFS2-5EBU].

[13] *E.g.*, Natasha Singer, *Flo settles F.T.C. charges of misleading users on privacy*, N.Y. TIMES (Jan. 13, 2021), https://www.nytimes.com/2021/01/13/business/flo-privacy.html?smid=url-share [https://perma.cc/3MM9-CXFS]; Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REPORTS (Sept. 17, 2020), https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/ [https://perma.cc/VSB2-WLV7].

[14] *See generally* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.) (protecting entities and data relevant to 1996, leaving uncovered many recent digital healthcare developments).

[15] *See* Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, SCI., at 447, 453 (2019).

Section V provides a number of legislative requirements necessary for any regulation to adequately respond to the digital health revolution.

II. BIG TECH'S EXPANSION INTO HEALTHCARE INDUSTRIES

[7] In just the last few years, Big Tech companies have revolutionized the healthcare industry. To accomplish this, firms have repurposed a familiar playbook used in other industries for the highly lucrative healthcare sector. Specifically, these companies are transforming the healthcare economy by (1) developing hardware and software designed to constantly collect medical data; (2) inferring medical information from seemingly non-health related consumer data; (3) partnering with hospital and medical practitioners to develop machine learning and AI capabilities in exchange for patient medical records; and (4) acquiring medical startups to build out information collection infrastructures and to amass existing troves of personal health data.

A. Developing Hardware and Software Designed to Collect Health Data

[8] Foundational to Big Tech's entrance into the healthcare sector has been the explosion of wearable technology.[16] Wearable technology is not new. As early as 1996, Dr. Sungmee Park and Dr. Sundaresan Jayaraman created the Smart Shirt, the first "intelligent" wearable device, as a DARPA-funded combat technology.[17] Professional athletes have also tracked personal metrics for decades, seizing on any way to gain an edge over

[16] *See The Explosion of Wearable Sensors in Healthcare*, WHATNEXT (Dec. 11, 2020), https://www.whatnextglobal.com/post/wearable-sensors-in-healthcare [https://perma.cc/TVQ9-UC2D].

[17] Sungmee Park & Sundaresan Jayaraman, *Enhancing the Quality of Life Through Wearable Technology*, IEEE ENG'G MED. & BIOLOGY MAG., May–June 2003, at 41, 42.

competitors.[18] Researchers envisioned wearable technology as a way to enhance quality of life and profoundly reshape the healthcare system.[19]

[9] While it may have started as a niche industry, wearable tech is now decidedly mainstream, and Big Tech has both contributed to and benefited from its expansive use. For example, some companies have exploited their existing surveillance capabilities to monitor health data. Indeed, the iPhone's built-in accelerometer and GPS can now be used as a pedometer to track users' steps.[20] But the real revolution has been in the proliferation of new hardware specifically designed to track and monitor user health data.

[10] Tech firms compete to develop smartwatches with the most sophisticated health-monitoring capabilities. Apple describes its Apple Watch as the "ultimate guardian for your health,"[21] as the device tracks blood oxygen levels, heartrate, and sleep patterns.[22] Amazon's Halo bracelet purports to measure body fat by having users take and scan 3D pictures of themselves in their underwear,[23] and detects a user's emotional

[18] *See* Yewande Adesida et al., *Exploring the Role of Wearable Technology in Sport Kinematics and Kinetics: A Systematic Review*, 19 SENSORS, no. 7, 2019, at 1, 2.

[19] *See* Paul Lukowicz et al., *Wearable Systems for Health Care Applications*, 43 METHODS INFO. MED. 232, 233, 235 (2004).

[20] Daniel N. Martin, *How to Use Your iPhone as a Pedometer*, LIFEWIRE (Oct. 22, 2020), https://www.lifewire.com/use-iphone-as-pedometer-4776496 [https://perma.cc/3NHX-NJ5U].

[21] Rachel Kraus, *The Apple Watch Series 4 finally goes edge-to-edge*, MASHABLE (Sept. 12, 2018), https://mashable.com/article/apple-watch-series-4-apple-event-2018/ [https://perma.cc/3MAJ-9XLZ].

[22] Mitroff, *supra* note 6; Lance Whitney, *How to Monitor Your Heart Rate With an Apple Watch*, PCMAG (Nov. 2, 2020), https://www.pcmag.com/how-to/how-to-monitor-your-heart-rate-with-the-apple-watch [https://perma.cc/3NRP-LBUP].

[23] Dieter Bohn, *Amazon Announces Halo, A Fitness Band and App That Scans Your Body and Voice*, VERGE (Aug. 27, 2020, 9:00 AM), https://www.theverge.com/2020/8/27/21402493/amazon-halo-band-health-fitness-body-scan-tone-emotion-activity-sleep [https://perma.cc/YS78-ZL78].

state by listening to the wearer's voice.[24] Halo users are encouraged to participate in purportedly "science-backed Labs," which score individuals based on metrics like "sleep efficiency."[25] Fitbit monitors skin temperature and breathing rates.[26] Bleeding-edge research has developed watch-sized devices that can monitor glucose, lactate, pH, and electrolytes by analyzing a user's sweat.[27]

[11] Smartwatches are just the beginning. Headbands can record brainwave patterns while users sleep or meditate.[28] Google's Project Amber is developing hardware to read EEG's for biomarkers of depression.[29] Apple offers blood glucose monitoring kits that come with lancing devices and test strips.[30] Other devices measure a person's metabolism by tracking

[24] *Id.* at 9 (listing emotional states such as hopeful, elated, hesitant, bored, happy, and worried).

[25] Chris Smith, *Amazon Halo review: Super intrusive but big-brand Labs shine through*, WAREABLE (Dec. 22, 2020), https://www.wareable.com/fitness-trackers/amazon-halo-review-8244 [https://perma.cc/8UTM-EQN3].

[26] Ethan Watters, *What Temperature Reveals Isn't Just Skin Deep*, FITBIT BLOG (Nov. 16, 2020), https://blog.fitbit.com/track-your-skin-temperature/ [https://perma.cc/FWA3-2KRJ].

[27] Charles Hall, *Wristwatch' Monitors Body Chemistry to Boost Athletic Performance, Prevent Injury*, N.C. ST. UNIV. ELEC. & COMPUT. ENG'G (Feb. 5, 2020), https://ece.ncsu.edu/2020/02/wristwatch-monitors-body-chemistry-to-boost-athletic-performance-prevent-injury/ [https://perma.cc/9NHR-6LP8].

[28] *A Deep Dive into Brainwaves: Brainwave Frequencies Explained*, MUSE (June 25, 2018), https://choosemuse.com/blog/a-deep-dive-into-brainwaves-brainwave-frequencies-explained-2/ [https://perma.cc/EB5Q-AV8X] (describing how brainwaves can be detected by placing electrodes on the scalp).

[29] Obi Felten, *Sharing Project Amber with the mental health community*, MEDIUM: BLOG X CO. (Nov. 2, 2020), https://blog.x.company/sharing-project-amber-with-the-mental-health-community-7b6d8814a862 [https://perma.cc/YCB2-33KJ].

[30] *One Drop Chrome Blood Glucose Monitoring Kit*, APPLE, https://www.apple.com/shop/product/HMN02LL/A/one-drop-chrome-blood-glucose-monitoring-kit [https://perma.cc/AP4G-QAGR].

carbon dioxide in breath.[31] Biosensors printed directly on skin can accurately measure body temperature, skin moisture, and electrophysiological signals.[32] Smart pills and ingestible sensors can communicate via Bluetooth to deliver drugs, predict infections, and treat diseases.[33] These new devices offer companies ways to constantly track users and collect health data in ways that were previously unavailable.

[12] Another turf war exists in the voice assistant market, as tech companies simultaneously fight for control over people's homes while also designing new voice-enabled medical applications. A recent update to Apple's Siri allows users to have back-and-forth conversations about health problems.[34] Amazon has partnered with Boston's Children Hospital, Atrium Health, the National Health Service (NHS), and other hospitals to allow

[31] *The Technology Used in Labs, Now at Your Fingertips*, LUMEN, https://www.lumen.me/how-it-works [https://perma.cc/Z9JB-Q3JT].

[32] Helen Albert, *Biosensors Printed Directly on Skin Bring Wearable Tech to Next Level*, FORBES (Oct. 24, 2020, 10:00 AM), https://www.forbes.com/sites/helenalbert/2020/10/24/biosensors-printed-directly-on-skin-bring-wearable-tech-to-next-level/?sh=54f4361937d3 [https://perma.cc/S6GH-52CN].

[33] Elise Reuter, '*Smart Pill' startup etectRx strikes partnership with Pear Therapeutics*, MEDCITY NEWS (Jan. 14, 2021, 1:47 PM), https://medcitynews.com/2021/01/smart-pill-startup-etectrx-strikes-partnership-with-pear-therapeutics/ [https://perma.cc/T9BX-6AAY]; Anne Trafton, *Ingestible Capsule Can Be Controlled Wirelessly*, MIT NEWS (Dec. 13, 2018), https://news.mit.edu/2018/ingestible-pill-controlled-wirelessly-bluetooth-1213 [https://perma.cc/KPM3-EJLA].

[34] Alex Hern, *Apple made Siri deflect questions on feminism, leaked papers reveal*, GUARDIAN (Sept. 6, 2019, 8:00 AM), https://www.theguardian.com/technology/2019/sep/06/apple-rewrote-siri-to-deflect-questions-about-feminism [https://perma.cc/8QPQ-ATWQ].

patients to use Alexa to access their health data by voice.[35] Users can ask Alexa to "refill my medication," "schedule an appointment," and "start my daily check in."[36] The Mayo Clinic's Alexa-enabled program can deliver first aid instructions to patients, and has even studied voice data to diagnose cardiovascular disease.[37] Other companies believe a user's voice, tone, and clarity could predict psychotic episodes and strokes.[38] Doctors suggest that voice activated tools can help the elderly, blind, and those who otherwise cannot access a computer. [39] Each new development presents technology companies with a new stream of healthcare data.

[13] Beyond hardware, new health and wellness apps allow users to directly input medical information. These apps both collect data and provide health-based behavioral nudges.[40] For example, the Calm app aims to improve users' "mental fitness" by tracking their mood, sleep, and

[35] Heather Landi, *Healthcare network rolls out voice-enabled digital assistant across 1,500 practices*, FIERCE HEALTHCARE (June 12, 2019, 12:27 pm), https://www.fiercehealthcare.com/tech/healthcare-network-rolls-out-voice-enabled-digital-assistant-across-1-500-practices [https://perma.cc/M8VR-QUXX]; Rachel Jiang, *Introducing New Alexa Healthcare Skills*, AMAZON: ALEXA DEVELOPER (Apr. 4, 2019), https://developer.amazon.com/en-US/blogs/alexa/alexa-skills-kit/2019/04/introducing-new-alexa-healthcare-skills [https://perma.cc/KP9E-HLDL].

[36] *Voice for Healthcare*, AMAZON: ALEXA DEVELOPER, https://developer.amazon.com/en-US/alexa/alexa-skills-kit/get-deeper/custom-skills/healthcare-skills [https://perma.cc/VS88-3S4T].

[37] Ross, *supra* note 6.

[38] *Id.*

[39] *See Alexa Together*, AMAZON, https://www.amazon.com/b/ref=ods_surl_ac?&node=21390531011 [https://perma.cc/A8Q3-CVYT].

[40] *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (Penguins Books, 2019) (discussing nudges); Neil Shah & Srinath Adusumalli, *Nudges and the Meaningful Adoption of Digital Health*, 17 PERSONALIZED MED. 429, 430 (2020) (discussing nudges in digital healthcare).

meditation practice.[41] The app also sends users daily reminders and provides statistical feedback to steer and improve their sleep and meditation habits.[42] Period-tracking apps monitor user mood changes, body temperature, and cycle to best predict fertility windows to help users become pregnant.[43] Apple and Google have also developed health hubs that connect with, and receive data from, other health and wellness apps.[44] These hubs also sync with other hardware in the ecosystem like the Apple Watch.[45] Users can manually add data like their height and weight, the last time they had sex, and time spent brushing their teeth.[46] The Apple Health app can also sync patient electronic health records (EHR) to store immunization records, lab results, medications, and past procedures.[47] Through the Apple Health app, any health system or clinic can register to enable patients to

[41] Amanda Hess, *The App That Tucks Me in at Night*, N.Y. TIMES (July 17, 2019), https://www.nytimes.com/interactive/2019/07/17/arts/calm-app-sleep-meditation.html [https://perma.cc/E2FR-U2RZ].

[42] Nancy A. Haug, *Calm: A Professional Review*, ONE MIND PSYBER GUIDE (Jan. 6, 2017), https://onemindpsyberguide.org/expert-review/calm-professional-review/#ProductDescription [https://perma.cc/2JGT-56S8].

[43] Melissa Willets, *The 8 Best Period and Ovulation Tracker Apps for Getting Pregnant*, PARENTS, https://www.parents.com/getting-pregnant/ovulation/fertile-days/the-10-best-period-and-ovulation-tracker-apps/ [https://perma.cc/SRN4-A9HH]; Daniel A. Epstein et al., *Examining Menstrual Tracking to Inform the Design of Personal Informatics Tools*, ASS'N FOR COMPUTING MACH. (CHI Conf. on Hum. Factors Computing Sys., Denver Colorado.), May 6–11, 2017, at 6876, 6880.

[44] GOOGLE FIT, https://www.google.com/fit/ [https://perma.cc/AWQ9-GYP6]; *The Health App*, APPLE, https://www.apple.com/ios/health/ [https://perma.cc/Y6NG-KLAR].

[45] *Manage Health data on your iPhone, iPod Touch, or Apple Watch*, APPLE (May 20, 2020), https://support.apple.com/en-us/HT204351 [perma.cc/2NA6-6BCX].

[46] *See id.*

[47] *Empower Your Patients with Their Health Data*, APPLE, https://www.apple.com/healthcare/health-records/ [https://perma.cc/RX8U-JWEZ].

download their EHRs.[48] More than collecting data and allowing for manual data entry, these apps also incorporate gamification elements to engage and motivate users to accomplish fitness goals.[49]

[14] Never before have firms had access to such sensitive information, much of which is constantly collected and continuously updated. Nor does development—or consumer demand—seem to be slowing down.[50]

B. Collecting and Monetizing of Healthcare Data and Emergent Medical Data

[15] In addition to developing new proprietary devices and software applications for medical data collection, Big Tech gathers user healthcare information through the more familiar technique of third-party data collection.[51] Users often do not know their medical information is being shared with companies like Google and Facebook. While troubling, these practices should come as no surprise in today's informational-capitalist

[48] Ricky Bloomfield (@rickybloomfield), TWITTER (June 26, 2019, 9:26 PM), https://twitter.com/rickybloomfield/status/1144054462408998912 [perma.cc/7CFW-V6PG].

[49] Alex Shestel, *Gamification in Healthcare: The Value of Fun*, BELITSOFT (Apr. 23, 2020), https://belitsoft.com/custom-application-development-services/healthcare-software-development/gamification-in-healthcare-just-for-fun-or-has-real-value [perma.cc/6FTF-JWDH]; Dominic King et al., *'Gamification': Influencing Health Behaviours with Games*, 106 J. ROYAL SOC'Y MED. 76, 76–77 (2013).

[50] Shaun Callaghan et al., *Feeling good: The future of the $1.5 trillion wellness market*, MCKINSEY & CO. (Apr. 8, 2021), https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/feeling-good-the-future-of-the-1-5-trillion-wellness-market [https://perma.cc/K479-7ZQU].

[51] *See, e.g.*, Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019, 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 [perma.cc/E8H6-7BFG].

landscape.[52] More jarring, and equally difficult to address, are recent developments in data analytics that allow medical insights and inferences from seemingly non-medical information, like social media posts.[53]

1. Third-party Sharing of Health Information

[16] Tech titans receive mountains of medical data from third-party applications. App developers use software development kits (SDKs) to integrate certain functions to better understand user behavior.[54] Information stored in an app that uses SDK code can be passed along to the SDK maker.[55] Facebook has some of the most popular SDKs, meaning much of the healthcare data collected through applications using SDKs may be passed on to Facebook. Of the top 1,000 apps in Apple's App Store and the Google Play Store, 17.6% and 25.4% respectively had at least one Facebook SDK.[56] In 2019, at least six of the top fifteen health and fitness apps were found to have shared sensitive personal information with Facebook.[57] Two of the most popular menstruation apps, MIA Fem and Maya shared information with Facebook about users' contraception use, alcohol consumption, masturbation habits, and period timing.[58] Maya started

[52] *See generally* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 5–7 (Oxford University 2019) (describing the transition of political economies towards informational capitalism).

[53] *See id*.

[54] Schechner & Secada, *supra* note 51.

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data*, PRIVACY INT'L (Sept. 9, 2019), https://www.privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data [perma.cc/7R9K-VB8G].

sharing data with Facebook even before users agreed to its privacy policy.[59] Better Me, a home workout and diet app, shares user-reported height and weight with Facebook.[60] Symptom checking websites like WebMD share user data with Google's Double Click, Amazon, Facebook, and Microsoft.[61] While sharing medical information with Facebook technically violates the company's terms of service, Facebook has taken no steps to enforce the policy and still actively profits from health information shared with the company through third parties.[62]

[17] In many respects, these sharing protocols are business as usual for tech companies.[63] But medical information is particularly sensitive, and the sharing of healthcare data is highly regulated in traditional healthcare contexts.[64] Users would therefore be reasonable in assuming that information about their sex life will not immediately be shared with third parties. Apple CEO Tim Cook, in the midst of his company's foray into healthcare, has called privacy a fundamental right, and views privacy as a competitive edge.[65] While commendable, the above demonstrates that

[59] *Id.*

[60] Schechner & Secada, *supra* note 51.

[61] Madhumita Murgia & Max Harlow, *How top health websites are sharing sensitive data with advertisers*, FIN. TIMES (Nov. 12, 2019), https://www.ft.com/content/0fbf4d8e-022b-11ea-be59-e49b2a136b8d [https://perma.cc/M7EV-6U9B].

[62] N.Y. STATE DEP'T FIN. SERVS., REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS 16 (2021).

[63] Schechner & Secada, *supra* note 51.

[64] *See infra* Section IV.

[65] *Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right'*, NPR: ALL TECH CONSIDERED (Oct. 1, 2015, 6:17 PM), https://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right [https://perma.cc/Z6KV-4PFC]; Laura Sydell, *Storing Health Records On Your Phone: Can Apple Live Up To Its Privacy Values?*, NPR: ALL TECH CONSIDERED (Feb. 27, 2019, 2:55 PM), https://www.npr.org/2019/02/27/697026827/storing-health-records-on-your-phone-can-apple-live-up-to-its-privacy-values [https://perma.cc/KPN4-YNMS].

health apps do not always live up to their privacy guarantees. Under the current regulatory model, this privacy promise can feel more aspirational and brand-driven than a reflection of reality.

2. Linking and Inferring Healthcare Data

[18] Under the informational capitalist regime, data's value comes not from the collection itself, but rather from inferences that can be made from the data.[66] Context and patterns gleaned from data are valuable for their predictive power.[67] These inferences also drive the lucrative practice of targeted ads.[68] The more data collected, the more accurate these inferences become, increasing the value of the resulting predictions.[69] These mechanisms apply with equal force in healthcare contexts. Some applications are straightforward: if a user searches for the best treatment for a cough, sore throat, or congestion, Google may infer that the user has a cold. If a Facebook user joins a breast cancer support group, Facebook may assume that the user has breast cancer.[70] But recent advances in machine learning also allow for medical inferences from less intuitive non-medical data sets.

---

[66] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 95–96 (2019).

[67] *Id.*

[68] *See id.* at 93–94.

[69] COHEN, *supra* note 52, at 49 (2019) ("The technologies of the sensing net are designed to modulate surveillant attention, offering options tailored to what is known or inferred about data subjects' habits, beliefs, and inclinations. As social psychologist Shoshana Zuboff explains, that goal demands ever more detailed behavioral patterning. To achieve maximum accuracy and minimum uncertainty, the sensing net must plumb the depths of users' experiences, interpreting minute behavioral cues to ferret out underlying cognitive and emotional patterns.").

[70] Kate Fazzini & Christina Farr, *Facebook recently closed a loophole that allowed third parties to discover the names of people in private, 'closed' Facebook groups*, CNBC (Aug. 1, 2018, 3:59 PM), https://www.cnbc.com/2018/07/11/facebook-private-groups-breast-cancer-privacy-loophole.html [https://perma.cc/DLZ3-2DT7].

[19] Early attempts at more sophisticated health inferences were unsuccessful. Beginning in 2008, Google leveraged vast troves of search data to try to detect influenza outbreaks at an early stage.[71] Google Flu Trends was ultimately a disappointment—it failed to detect the 2009 flu and overestimated the 2012–2013 peak—and eventually, the service shut down.[72] The predictive potential of medical inferences, however, was recognized.[73] Now, companies use data to make predictions that once seemed impossible. Facebook analyzes posts, videos, and livestreams to determine whether users may be at risk for suicide by giving risk scores to individual words or phrases.[74] Instagram filters and Twitter posts can be used to predict depression.[75] New machine-learning techniques estimate drug use based on Facebook likes and status updates.[76] Microsoft

[71] Jeremy Ginsberg et al., *Detecting Influenza Epidemics Using Search Engine Query Data*, 457 NATURE 1012, 1012–14 (2009).

[72] Donald R. Olson et al., *Reassessing Google Flu Trends Data for Detection of Seasonal and Pandemic Influenza: A Comparative Epidemiological Study at Three Geographic Scales*, 9 PLOS COMPUTATIONAL BIOLOGY, no. 10, 2019, at 1, 3–4.

[73] David Lazer & Ryan Kennedy, *What We Can Learn From the Epic Failure of Google Flu Trends*, WIRED (Oct. 10, 2015, 7:00 AM), https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/ [https://perma.cc/656T-Z7Z3].

[74] Mason Marks, *Artificial Intelligence-Based Suicide Prediction*, 21 YALE J.L. & TECH. 98, 108 (2019); Jacqueline Howard, *Facebook screens posts for suicide risk, and health experts have concerns*, CNN (Feb. 12, 2019, 10:18 AM), https://www.cnn.com/2019/02/11/health/facebook-suicide-prevention-questions/index.html [https://perma.cc/TL8W-ZXEL].

[75] Andrew G. Reece & Christopher M. Danforth, *Instagram Photos Reveal Predictive Markers of Depression*, 6 EPJ DATA SCI. 1, 1–2 (2017); Moin Nadeem et al., Identifying Depression on Twitter 1, 3, 8 (2016) (unpublished manuscript) (on file with authors).

[76] Tao Ding et al., Social Media-based Substance Use Prediction 1 (May 1, 2017) (unpublished manuscript) (on file with authors).

researchers have used Bing search results, mouse tracking, and keyboard strokes to predict if users have Parkinson's Disease.[77]

[20] A recent study found Facebook posts can be strong predictors of diabetes, pregnancy, anxiety, and psychoses.[78] The study also associated certain topics with diseases. For instance, diabetes was linked with use of religious language like "Jesus" and "pray."[79] Finally, Google subsidiary Verily gives COVID-19 risk scores based on users' Google accounts and other personal information.[80]

[21] These new and expansive sources of healthcare information are known as Emergent Medical Data (EMD).[81] Whereas traditional medical information is obtained directly and voluntarily from patients, EMD is "synthesized from digital traces that people continuously shed through their daily interactions with technology."[82] However, while EMD shows promise, it also further blurs the line between medical and non-medical information. If mouse tracking and religious language can have healthcare implications, what data would not?

[77] Liron Allerhand et al., *Detecting Parkinson's Disease from Interactions with a Search Engine: Is Expert Knowledge Sufficient?*, ASS'N FOR COMPUTING MACH. (27th ACM Int'l Conf. on Info. & Knowledge Mgmt., Torino, It.), May 3, 2018, at 1–2.

[78] Raina M. Merchant et al., *Evaluating the Predictability of Medical Conditions from Social Media Posts*, 14 PLOS ONE 1, 4 (2019).

[79] *Id.* at 5.

[80] Jennifer Elias, *Alphabet's verily launches a limited coronavirus screening website*, CNBC (Mar. 16, 2020, 12:45 AM), https://www.cnbc.com/2020/03/15/alphabets-verily-says-it-will-launch-a-limited-coronavirus-testing-website-monday.html [https://perma.cc/2C55-4W6F]; *see* Marks, *supra* note 9, at 1006-07 (describing how Emergent Medical Data is mined and applied).

[81] Marks, *supra* note 9, at 1006.

[82] *Id.* at 1001.

[22] Health professionals, like tech companies, are increasingly turning to EMD to inform preventative health policy. Algorithmic tools like polysocial risk scores apply a Big Data approach to social determinants of health (SDOHs), which are the "environment[s] in which people are born, live, learn, play, work, and age."[83] Some believe that SDOHs offer maximum predictive power when viewed in the aggregate.[84] Polysocial risk scores would align with that belief, assessing health risks associated with "varying combinations of social conditions."[85] To be effective, these risk scores would require comprehensive, individualized information, such as income and education, identity factors like religion, sex, ethnicity, and other factors such as quality of housing, local crime levels, air and water quality, and access to food.[86] This information would inevitably come from large technology companies who already have troves of social data.[87]

[23] Polysocial risk scores show just how much sensitive health information is up for grabs. Seemingly nothing is off limits if accurate inferences can be made. As machine learning and algorithmic capabilities become more accurate at prediction and causal connection, the stronger the calls will be for extensive use of EMD to make medical inferences.

---

[83] *Determinants of Health*, OFF. DISEASE PREVENTION & HEALTH PROMOTION, https://www.healthypeople.gov/2020/about/foundation-health-measures/Determinants-of-Health#social [https://perma.cc/W6XC-Q3QG] (stating that examples of social determinants include "availability of resources to meet daily needs, such as educational and job opportunities, living wages, or healthful foods"; "social norms and attitudes, such as discrimination"; "exposure to crime, violence, and social disorder, such as the presence of trash"; "social support and social interactions"; "exposure to mass media and emerging technologies, such as the Internet or cell phones"; "socioeconomic conditions, such as concentrated poverty"; "quality schools"; "transportation options"; "public safety"; and "residential segregation").

[84] Jose F. Figueroa et. al., *Addressing Social Determinants of Health: Time for a Polysocial Risk Score*, 323 JAMA 1553, 1553 (2020).

[85] *Id.*

[86] *Id.*

[87] *See id.* at 1553–54.

C. Partnering with Hospitals and Healthcare Providers

[24] The third digital healthcare development stems from Big Tech's collaboration with traditional medical providers. This too can be seen as an extension of the traditional data bargain that tech firms offer. Whereas users provide data in exchange for personalization, hospitals offer patient data with the expectation of more efficient and effective healthcare tools. Tech companies exact this *quid pro quo* by developing algorithmic and machine learning tools specific to medical contexts, and by leveraging proprietary hardware like wearables for use in clinical studies.

1. Algorithmic and Machine Learning Tools in Traditional Medical Contexts

[25] New data-driven tools aim to improve a wide range of processes in traditional healthcare contexts. Some improvements are designed to increase physician quality of life. For example, notetaking is one of the most laborious and time-consuming aspects of the practice of medicine.[88] To address the problem, hospitals are turning to tech firms for a major overhaul of their medical documentation system. Google recently launched a machine learning tool, Healthcare Natural Language API, which "identifies medical insights in documents, automatically extracting knowledge about medical procedures, medications, body vitals, or medical conditions."[89] The API is meant to cut down on the time-consuming process of manual review of each document by healthcare professionals.[90] Amazon Comprehend Medical similarly uses machine learning to extract health data from medical

[88] *See* Christine Sinsky et al., *Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in 4 Specialties*, 165 ANNALS INTERNAL MED. 753, 753 (2016) ("For every hour physicians provide direct clinical face time to patients, nearly 2 additional hours is spent on EHR and desk work within the clinic day. Outside office hours, physicians spend another 1 to 2 hours of personal time each night doing additional computer and other clerical work.").

[89] Bodnari, *supra* note 11.

[90] *Id.*

text like doctor notes, clinical trial reports, and patient health records.[91] Other algorithmic innovations focus on detection and prevention of specific diseases; Amazon and Pittsburg Medical Center together use machine learning to study breast cancer, depression, and tumor growth;[92] Providence Hospital System is collaborating with Microsoft to develop a cancer-detecting algorithm using doctor notes in patient medical records;[93] Facebook's AI division is working with New York University School of Medicine to make MRI scans faster and more affordable.[94] Other developments involve migrating data to the cloud. EHR heavyweight Cerner is shifting much of its digital infrastructure to Amazon Web Services (AWS),[95] and the Mayo Clinic entered a deal with Google to do the same;[96] Providence will have Microsoft's cloud platform Azure host its clinical data;[97] Carnegie Mellon has partnered with University of Pittsburgh

[91] *Amazon Comprehend Medical*, AMAZON, https://aws.amazon.com/comprehend/medical/ [https://perma.cc/QN4H-5T55].

[92] *AWS and PHDA collaborate to produce more accurate machine learning models for breast cancer screening and depression*, AMAZON (Oct. 6, 2020), https://www.amazon.science/aws-and-phda-collaborate-to-produce-more-accurate-machine-learning-models-for-breast-cancer-screening-and-depression [https://perma.cc/493B-92RF].

[93] Evans, *supra* note 8.

[94] *See Facebook and NYU School of medicine launch research collaboration to Improve MRI*, FACEBOOK ENG'G (Aug. 20, 2018), https://engineering.fb.com/2018/08/20/ai-research/facebook-and-nyu-school-of-medicine-launch-research-collaboration-to-improve-mri/ [https://perma.cc/B27H-5A2H].

[95] Heather Landi, *Cerner senior exec: Amazon cloud partnership is driving Cerner's shift to become digital platform company*, FIERCE HEALTHCARE (Sept. 16, 2020, 7:15 AM), https://www.fiercehealthcare.com/tech/amazon-cloud-partnership-cerner-moving-beyond-ehrs-to-become-digital-platform-company [https://perma.cc/UU96-B7R3].

[96] Duska Anastasijevic, *Mayo Clinic selects Google as strategic partner for health care innovation, cloud computing*, MAYO CLINIC (Sept. 10, 2019), https://newsnetwork.mayoclinic.org/discussion/mayo-clinic-selects-google-as-strategic-partner-for-health-care-innovation-cloud-computing/ [https://perma.cc/AT7G-JUPD].

[97] MICROSOFT NEWS CTR., *supra* note 8.

Medical Center to leverage medical records, genomic sequencing, insurance records, and wearable data for use in theranostics and imaging systems.[98]

[26] In these partnerships, patient medical records serve as both raw materials and digital currency. To have any predictive insights, machine learning algorithms must be trained using vast amounts of health records.[99] As a result, healthcare providers fork over treasure troves of patient data in exchange for the promise of better tools. Ascension, the second-largest health system in the country, gave Google access to the records of its fifty million patients as part of a move to Google's cloud computing system, triggering a federal inquiry.[100] As a result, Google gained access to information such as patient names, dates of birth, lab tests, doctor diagnoses, billing claims, and medication and hospitalization histories.[101] Ascension did not notify patients that their information was being shared in this way.[102] Google struck a similar deal with the Mayo Clinic, gaining access to over ten million patient records.[103] As part of a project with University of Chicago Medical Center, Google was given access to EHR that contained the dates of patients' medical procedures.[104] This data, while perhaps necessary for machine learning insights, has value well beyond its use as a training tool. Identifiable patient information can be matched with user profiles and inform targeted ads. Even deidentified, aggregated patient data

[98] Ken Walters et al., *CMU, Pitt, UPMC Form Alliance to Transform Health Care Through Big Data*, CARNEGIE MELLON UNIV. (March 16, 2015), https://www.cmu.edu/news/stories/archives/2015/march/health-data-alliance.html [https://perma.cc/GCF5-J3E7].

[99] *See* Abhimanyu S. Ahuja, *The Impact of Artificial Intelligence in Medicine on the Future Role of the Physician*, 7 PEERJ, Oct. 2019, at 2, 6.

[100] Copeland & Needleman, *supra* note 8.

[101] *Id.*

[102] *Id.*

[103] Copeland et al., *supra* note 3.

[104] *Id.*

can be lucrative for advertising. Facebook recently asked a number of hospitals for anonymized patient data like illnesses and prescription info with the intent of pairing the information with Facebook's own collected user data.[105] "Facebook's pitch . . . was to combine what a health system knows about its patients (such as: person has heart disease, is age 50, takes 2 medications and made 3 trips to the hospital this year) with what Facebook knows (such as: user is age 50, married with 3 kids, English isn't a primary language, actively engages with the community by sending a lot of messages)."[106] Thus, collaborations with healthcare providers reinforce and enhance Big Tech's practices of linking and inference. Algorithmic tools trained on EHR and other medical records offer yet another comprehensive stream of data which Big Tech can use to bolster its predictive power, not just in medical contexts, but in all sectors in which they compete.

2. Using Proprietary Devices in Hospitals and Clinical Studies

[27] As discussed above, new medical hardware offers companies countless opportunities for patient monitoring and medical data collection.[107] Hospitals and medical providers are eager to capitalize on new opportunities to track patients and improve care.[108] Tech companies, in turn,

[105] Christina Farr, *Facebook sent a doctor on a secret mission to ask hospitals to share patient data*, CNBC (Apr. 6, 2018, 11:46 AM), https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html [https://perma.cc/W3BX-8XHA].

[106] *Id.*

[107] *See supra* Section II.

[108] *See* Michelle L'Hommedieu et al., *Lessons Learned: Recommendations For Implementing a Longitudinal Study Using Wearable and Environmental Sensors in a Health Care Organization*, 7 JMIR MHEALTH UHEALTH, no. 12, 2019, at 1 ("Although traditional methods of data collection in naturalistic settings can shed light on constructs of interest to researchers, advances in sensor-based technology allow researchers to capture continuous physiological and behavioral data to provide a more comprehensive understanding of the constructs that are examined in a dynamic health care setting.").

are eager to gain a stronger foothold in the medical industries and fine-tune their proprietary technologies.[109] Given this incentive structure, it is not surprising that a number of commercial partnerships using new data-driven hardware have emerged. Some healthcare providers encourage their patients to buy wearable technologies by offering discounts: through a partnership with Cerner, Amazon Halo customers can share health data directly with their healthcare providers;[110] Life insurer John Hancock offers customers free Halo devices in exchange for their medical data;[111] Fitbit has partnered with Blue Cross Blue Shield and United Healthcare to offer discounts and incentives in exchange for user data.[112]

[28] Other partnerships focus on specialized research of particular ailments and diseases. Apple has partnered with a number of hospitals to test the Apple Watch's tracking capabilities. In a study with Anthem, Apple used its smartwatch to monitor the symptoms of 900 patients with asthma.[113] The Apple Watch tracked patient heart rate and blood oxygen level.[114] The study was designed to test whether the Apple Watch could accurately predict and prevent asthma attacks based on digital

[109] *See* Hemant Taneja, *How Tech Companies Can Help Fix U.S. Health Care*, HARV. BUS. REV. (Apr. 28, 2020), https://hbr.org/2020/04/how-big-tech-can-help-fix-u-s-health-care [https://perma.cc/H57H-XUV7].

[110] Landi, *supra* note 95.

[111] Emily Mullin, *Want a Free Amazon Halo? Just Hand Over Your Data to This Insurance Company*, ONEZERO (Aug. 28, 2020), https://onezero.medium.com/want-a-free-amazon-halo-wearable-just-hand-over-your-data-to-this-major-insurance-company-56b6430b0749 [https://perma.cc/9V33-W97Y].

[112] *See* Victoria Song, *Guys, Fitbit Started Profiting Off Health Data Long Before Google Showed Up*, GIZMODO (Nov. 19, 2019, 3:20 PM), https://gizmodo.com/guys-fitbit-started-profiting-off-health-data-long-bef-1839940074 [https://perma.cc/46MH-MN2Z].

[113] Elise Reuter, *Apple launches asthma study with Anthem*, MEDCITY NEWS (Sept. 16, 2020, 8:41 PM), https://medcitynews.com/2020/09/apple-launches-asthma-study-with-anthem/ [https://perma.cc/6NHX-KZ6F].

[114] *Id.*

biomarkers.[115] The Apple Watch was also used in a Stanford University School of Medicine experiment to test the device's ability to detect irregular heartbeats and atrial fibrillation.[116] Along with the Harvard School of Public Health and the NIH, Apple launched a long-term study on menstrual cycles and gynecological conditions.[117] Medical researchers have also used Fitbits to detect falls and study obesity.[118]

[29] These examples demonstrate the symbiotic relationship between Big Tech and medical practitioners. Sensors and tracking devices give unprecedented access to patients. In return, the tools' health functions are tested and fine-tuned, legitimizing them as medical diagnostic devices.

D. Acquiring Healthcare Companies

[30] The final cornerstone of Big Tech's healthcare encroachment involves yet another familiar step: acquisition. Over the past two decades, tech titans have bought hundreds of start-ups, often to accomplish two goals: expand digital infrastructure and gain access to existing data stockpiles. Facebook acquired Connect U, Friendster, Instagram, and WhatsApp to both growth its social media and messaging empire and obtain

[115] *See id.*

[116] Marco V. Perez et al., *Large-Scale Assessment of a Smartwatch to Identify Atrial Fibrillation*, 381 NEW ENG. J. MED. 1909, 1910–11 (2019).

[117] *Apple announces three groundbreaking health studies*, APPLE: NEWSROOM (Sept. 10, 2019), https://www.apple.com/newsroom/2019/09/apple-announces-three-groundbreaking-health-studies/ [https://perma.cc/2BPA-48ME].

[118] *See, e.g.*, Samad Barri Khojasteh et al., *Improving Fall Detection Using an On-Wrist Wearable Accelerometer*, 18 SENSORS 1350, 1352 (2018); Scott W. Cheatham et al., *The Efficacy of Wearable Activity Tracking Technology as Part of a Weight Loss Program: A Systematic Review*, 58 J. SPORTS MED. & PHYSICAL FITNESS 534, 534–35 (2018); Erin E. Dooley et al., *Estimating Accuracy at Exercise Intensities: A Comparative Study of Self-Monitoring Heart Rate and Physical Activity Wearable Devices*, 5 JMIR MHEALTH UHEALTH, no. 3, 2017, at 1, 2.

the data of millions of users.[119] Google purchased YouTube, Motorola, Waze, DoubleClick, and Nest for the similar dual purpose.[120] Tech companies have pursued a similar strategy in the healthcare sector. Consider Google's purchase of Fitbit. Fitbit's value to Google was two-fold: The company offered a mountain of health data, plus the digital infrastructure to collect more.[121] Google has also acquired the intellectual property rights to Fossil's smartwatch capabilities.[122] Other companies have used the same tactic. Amazon purchased PillPack to kick-start its entrance into the prescription pharmacy industry,[123] Body Labs, a company that models and scans human bodies,[124] and Health Navigator, an online symptom checker

[119] Mark Glick and Catherine Ruetschlin, *Big Tech Acquisitions and the Potential Competition Doctrine: The Case of Facebook* 57–58 (Instit. New Econ. Thinking, Working Paper No. 104, 2019), https://www.ineteconomics.org/uploads/papers/WP-104-Glick-and-Reut-Oct-10.pdf [https://perma.cc/53E5-ET56].

[120] *See* ZUBOFF, *supra* note 66, at 151 ("What Google couldn't build, it bought.").

[121] *See, e.g.*, Patrick Lucas Austin, *The Real Reason Google is Buying Fitbit*, TIME (Nov. 4, 2019, 3:17 PM), https://time.com/5717726/google-fitbit/ [https://perma.cc/LUT5-HSN8]; Lauren Goode, *What Google's Fitbit Buy Means for the Future of Wearables*, WIRED (Nov. 2, 2019, 7:00 AM), https://www.wired.com/story/google-fitbit-future-of-wearables/ [https://perma.cc/7BKC-4Y98]; Bohn, *supra* note 7.

[122] Statt, *supra* note 7.

[123] Christina Farr & Annie Palmer, *Amazon jumps into the pharmacy business with online prescription fulfillment, fee delivery for Prime members*, CNBC (Nov. 17, 2020, 4:06 PM), https://www.cnbc.com/2020/11/17/amazon-pharmacy-free-prescription-delivery-for-prime-members.html [https://perma.cc/NAK9-GLXL]; Christina Farr, *The inside story of why Amazon bought PillPack in its effort to crack the $500 billion prescription market*, CNBC (May 13, 2019, 12:12 PM), https://www.cnbc.com/2019/05/10/why-amazon-bought-pillpack-for-753-million-and-what-happens-next.html [https://perma.cc/P38T-MCGY].

[124] Natasha Lomas & Jordan Crook, *Amazon has acquired 3D body model startup, Body Labs, for $50M-$70M*, TECHCRUNCH (Oct. 3, 2017, 2:54 PM), https://techcrunch.com/2017/10/03/amazon-has-acquired-3d-body-model-startup-body-labs-for-50m-70m/ [https://perma.cc/85BZ-WW37].

and triage tool.[125] Microsoft acquired Nuance, a company that develops medical speech and text machine learning tools, for $16 billion.[126] Finally, Apple bought small start-up Tueo Health to help integrate an asthma detection tool into its Apple Watch.[127]

[31] In just a few short years, Big Tech has completely disrupted traditional healthcare industries. Through the creation of medical monitoring devices, collection and analysis emergent medical data, partnerships with medical providers, and acquisitions of health starts ups, firms have ushered in a rapidly evolving era of digital health. The new data-driven regime is decentralized in nature and relies on constant monitoring and machine learning. These changes parallel characteristics of the familiar Big Data and Big Tech paradigms that have affected countless other sectors of the economy. But the healthcare industry is unique, and the sensitivity of medical data brings about greater scrutiny of these developments compared to other industries. This is certainly not to say that these data-driven medical innovations should be immediately dismissed or rejected. In fact, as the next Section of this Article discusses, many stakeholders have been eager to welcome this new era.

III. The Allure of the New Health Paradigm and its Exploitation by Big Tech

[32] The rise of digital healthcare tools can only be explained by the devices' immense value to industry participants. For individuals, self-tracking through apps and wearable technology offers the possibility of "self-knowledge through numbers"—a mantra with roots in the Quantified

[125] Christina Farr, *Amazon acquires start-up Health Navigator, its first health-related purchase since PillPack*, CNBC (Oct. 23, 2019, 5:30 PM), https://www.cnbc.com/2019/10/23/amazon-acquires-digital-health-start-up-health-navigator.html [https://perma.cc/BZK6-MNPT].

[126] Michael J. de la Merced et al., *Microsoft to Buy Nuance for $16 Billion to Focus on Health Care Tech*, N.Y. TIMES (July 1, 2021), https://www.nytimes.com/2021/04/12/business/microsoft-nuance-artificial-intelligence.html [https://perma.cc/WL2L-3LTK].

[127] *See* Farr & Kovach, *supra* note 7.

Self movement.[128] Self-monitoring is seen as a means of self-improvement. By tracking and recording, consumers can improve their fitness, sleep, and overall health. For medical practitioners, the appeal of the healthcare revolution is even stronger. Data-driven devices stand to improve physician quality of life, reduce burnout, and allow for more face time with patients. Moreover, algorithmic and machine learning medical tools offer the possibility of better and more efficient care, which could save lives and reduce costs. Indeed, the life-and-death consequences of healthcare are unique. These tangible benefits make the promise of digital healthcare tools impossible to ignore, even in spite of their flaws. And all the while, tech companies have deftly seized on this validation to give their actions moral force and stave off attempts at oversight.

A. Benefits to Consumers

[33] While some data collection techniques are passive and often go unnoticed by users, many new Big Tech healthcare devices require substantial opt-in.[129] Smartwatches, voice assistants, headbands, and other hardware are both expensive and constantly monitoring. Health apps can require users to input and log their information daily. Given the burden these products create, why are they in such high demand?[130] The answer can be explained, at least in part, by the inherent value many users find in self-

[128] *What is Quantified Self?*, QUANTIFIED SELF, https://quantifiedself.com/about/what-is-quantified-self/ [https://perma.cc/9VYQ-R3AT].

[129] *See, e.g.*, Sydell, *supra* note 65.

[130] *See, e.g., Smartwatch Market Value Projected to Reach US$ 88.7 Billion by 2027: Acumen Research and Consulting*, INTRADO GLOB. NEWSWIRE (Feb. 11, 2021), https://www.globenewswire.com/news-release/2021/02/11/2174308/0/en/Smartwatch-Market-Value-Projected-To-Reach-Us-88-7-Billion-By-2027-Acumen-Research-And-Consulting.html [https://perma.cc/G3B2-3GQG] (smartwatch market); *Global Voice Assistant Market is Set to Reach USD 5.9 Billion by 2026, Observing a CAGR of 30.5% During 2020-2026: VynZ Research*, INTRADO GLOB. NEWSWIRE (May 27, 2020), https://www.globenewswire.com/news-release/2020/05/27/2039499/0/en/Global-Voice-Assistant-Market-is-Set-to-Reach-USD-5-9-Billion-by-2026-Observing-a-CAGR-of-30-5-during-2020-2026-VynZ-Research.html [https://perma.cc/T636-XEB8] (voice assistant market).

tracking.[131] This phenomenon has roots in the Quantified Self (QS) movement.

[34] QS started as the niche hobby of two *Wired* editors, Gary Wolf and Kevin Kelly.[132] The idea was simple: "self-knowledge through numbers."[133] According to Wolf, "numbers hold secrets that [we] can't afford to ignore, including answers to questions [we] have not yet thought to ask."[134] "If you want to replace the vagaries of intuition with something more reliable, you first need to gather data."[135] During the early stages of the QS movement, self-tracking required time-consuming manual data entry into spreadsheets and analysis employing user-made graphs.[136] Self-monitoring was a labor of love and fringe hobby. However, with progress in data collection and analysis—though still years before Fitbit and the Apple Watch were mainstream—QSers could more easily log and chart personal data. This self-tracking ethos extended to virtually every human practice or ritual, like after-lunch mood, REM sleep, and alcohol and caffeine intake.[137] QSers met

[131] *Why Apple Watch*, APPLE, https://www.apple.com/watch/why-apple-watch/ [https://perma.cc/22PK-LH86] (stating that Apple Watch allows users to check email, receive calls, and functions similarly to an iPhone, which shows that not all value from self-tracking products comes from their ability to monitor the individual).

[132] *See* Gary Wolf, *What Is the Quantified Self?*, QUANTIFIED SELF (Mar. 3, 2011) https://quantifiedself.com/blog/what-is-the-quantified-self/ [https://perma.cc/ZHK2-MXH4].

[133] QUANTIFIED SELF, *supra* note 128.

[134] Gary Wolf, *The Data-Driven Life*, N.Y. TIMES MAG. (Apr. 28, 2010), https://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html [https://perma.cc/6SMT-BQT4].

[135] *Id.*

[136] *See* Susannah Fox & Maeve Duggan, *Tracking for Health*, PEW RSCH. CTR. (Jan. 28, 2013), https://www.pewresearch.org/internet/2013/01/28/tracking-for-health/ [https://perma.cc/2NUT-3BFU].

[137] *Counting every moment*, ECONOMIST (Mar. 3, 2012), https://www.economist.com/technology-quarterly/2012/03/03/counting-every-moment [https://perma.cc/7MUT-EKX4].

at conferences and used industrial technology to collect and analyze personal health data for self-improvement.[138] The tenets of the movement echo those of high modernity, where data collection was thought necessary to better inform decision making and management.[139] But whereas high modernity focused on information collection to inform experts and society at-large, QS is decidedly more neoliberal. Here, data collection is decentralized and based on notions of self-care. For QSers, monitoring and recording is for the benefit of the individual alone.

[35] Then came Big Tech. Identifying an opportunity to both legitimize and increase data collection, tech companies embraced QS and made it mainstream. Just a decade ago, self-tracking was considered "wacky" and "strange."[140] Now, Big Tech markets products based on their ability to monitor the user.[141] By adopting the QS ethos and mass producing self-tracking devices, Big Tech has asserted itself as a third-party beneficiary to practices that were once individual in nature. From this perspective, it is not surprising that tech companies were quick to latch onto and exploit the QS movement, for it is just one of a handful of examples of Big Tech using

[138] *Id.*

[139] *See* Lisa Mendelman, *The Quantified Self*, 3 MODERNISM/MODERNITY (Jul. 7, 2018), https://modernismmodernity.org/forums/posts/quantified-self [https://perma.cc/42PY-UHNH] ("QS's origins are usually dated to the 1970s and the introduction of self-surveillance via wearable technology. However, I think the modernist period forms a crucial prehistory to this cultural movement. This era gave birth to the standardized models of physical and mental health that underpin our current notions of modern selfhood. It nurtured biopolitical phenomena like personal hygiene, psychoanalysis, self-help, and birth control into being.").

[140] Nic Fleming, *Know thyself: the Quantified Self devotees who live by numbers*, GUARDIAN (Dec. 2, 2011), https://www.theguardian.com/science/2011/dec/02/psychology-human-biology [https://perma.cc/E2DD-TJ8J].

[141] *See, e.g.*, *Track Your Sleep with Apple Watch*, APPLE SUPPORT, https://support.apple.com/guide/watch/sleep-apd830528336/watchos [https://perma.cc/8W44-A6FC].

neoliberalism and techno-libertarianism for its own financial gain.[142] Co-opting the QS movement increases the allure of the Big Tech bargain and strengthens the mandate for ubiquitous data collection.[143]

[36] That this new wave of techno-optimism could occur simultaneously with the ongoing "Techlash" is surprising.[144] Institutions and individuals alike still struggle to understand and grapple with the externalities that Big Data and Big Tech have on political discourse, privacy, discrimination, speech, and competition.[145] Yet, many are happy to continue accepting Big Tech's solutions to problems they did not know they had. Of course, not

[142] *See* ZUBOFF, *supra* note 66, at 340 ("Surveillance capitalism found shelter in the neoliberal zeitgeist that equated government regulation of business with tyranny. This 'paranoid style' favored self-management regimes that imposed few limits on corporate practices."); Cohen, *supra* note 52, at 103–04 ("The interlocking frames of the surveillance-innovation complex, the marketplace of ideas, and the information laboratory express a distinctively neoliberal ideology within which profit-motivated private enterprises are appropriate and morally virtuous guarantors of social progress, expressive liberty, and robust debate about matters of public importance.").

[143] COHEN, *supra* note 52, at 81–82 ("Predictably, however, commercial providers of QS technologies and applications entered the field . . . . As they have done so, the dialogue around QS has shifted, de-emphasizing control over data and emphasizing instead the need to provide and share data to gain tools for controlling other aspects of one's life, including health, diet, and fitness, but also work habits, sex life, sleep patterns, and so on."); EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM 234 (2013) ("In a way, the rise of self-tracking might reverse the debate on privacy: instead of worrying about companies tracking what we do online, why not do the very opposite and lament that so much of what we do online is not yet recorded . . . .").

[144] *See* KNIGHT FOUNDATION, TECHLASH? AMERICA'S GROWING CONCERN WITH MAJOR TECHNOLOGY COMPANIES 1, 3, 5 (2020), https://knightfoundation.org/wp-content/uploads/2020/03/Gallup-Knight-Report-Techlash-Americas-Growing-Concern-with-Major-Tech-Companies-Final.pdf [https://perma.cc/PN6P-PTRX].

[145] *See, e.g.*, *Permanent Suspension of @realDonaldTrump*, TWITTER BLOG (Jan. 8, 2021), https://blog.twitter.com/en_us/topics/company/2020/suspension.html [https://perma.cc/S77P-M3X9]; John D. McKinnon, *These Are the U.S. Antitrust Cases Facing Google, Facebook and Others*, WALL ST. J. (Dec. 17, 2020, 3:17 PM), https://www.wsj.com/articles/these-are-the-u-s-antitrust-cases-facing-google-facebook-and-others-11608150564 [https://perma.cc/Y7FB-735Q].

everyone has bought into the QS movement. Critics argue that this "data fetishism," in seeking to reduce and quantify all phenomena to numbers, ignores the "entire world of human, social and environmental complexity."[146] Moreover, the empirical value of self-tracking is still unknown. QS experimentation lacks double-blinding and oversight, and any perceived gains may simply be placebo.[147] Whatever the merits, the appeal of self-tracking and the QS movement has resonated with many and simultaneously offers Big Tech a new market to capitalize within.

B. Benefits to Healthcare Professionals

[37] Healthcare is different. But which way does that cut? On one hand, medical professionals and researchers argue that the importance of saving lives requires access to patient data and cutting-edge research tools. But medical information is at the core of human dignity and autonomy, which has led to a healthcare-privacy exceptionalism regime under U.S. law.[148] The intricacies of healthcare privacy exceptionalism are discussed more in Section III, and in Section IV, this Article offers a framework to untangle the different types of data collection. This Section will focus on the specific benefits that digital healthcare tools offer physicians and healthcare workers, followed by a discussion highlighting the unique moral force that undergirds health data collection, and how Big Tech has exploited it.

---

[146] Tamar Sharon & Dorien Zandbergen, *From Data Fetishism to Quantifying Selves: Self-Tracking Practices and the Other Values of Data*, 19 NEW MEDIA & SOC'Y 1695, 1698 (2017).

[147] *Counting Every Moment*, 402 ECONOMIST; LONDON 2, 3 (Mar. 2012) ("'With self-tracking you never really know whether it is your experiment that is affecting the outcome, or your expectations of the experiment,' says Nancy Dougherty, a self-tracking enthusiast who works as a hardware engineer at Proteus Biomedical . . . . She found that taking dummy pills labelled 'happy', 'calm', 'focus' and 'will power' had a noticeable impact, even though she knew they were placebos.").

[148] *See* Nicholas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y, L., & ETHICS 143, 148 (2017).

1. Saving Lives and Improving Physician Quality of Life

[38] Whatever the issues that pervades the data-driven approach to healthcare, the very real potential for improved care, treatment, and research cannot be ignored. Every year, patients die from avoidable mistakes.[149] Tracking and monitoring using Big Data can lead to quality and efficiency gains through better analysis and more effective treatment.[150] AI and machine learning tools offer new possibilities for disease prediction and detection efforts.[151] The Mayo Clinic described its partnership with Google as opening "a lot of doors that aren't available to us now."[152] New insights into risk factors that lead to disease, precision medicine and individualized patient care, real-time analysis of behavior changes, and early identification and intervention of high-risk and high-cost patients are all potential outcomes of a more efficient and productive data-driven healthcare system.[153]

[39] Beyond the direct potential to improve treatment, digital healthcare tools also stand to improve physician quality of life. EHR has promise to enhance patient care and professional satisfaction, but its current state is time-consuming and inefficient.[154] In a recent study, EHR received an "F"

[149] LINDA T. KOHN ET AL., TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM 26–35 (2000) (describing medical error as a leading cause of death and injury).

[150] Price & Cohen, *supra* note 2, at 38.

[151] *See supra* Part II.C.1.

[152] Heather Landi, *Mayo Clinic taps Google Cloud as strategic partner to accelerate innovation in ai, analytics and digital tools*, FIERCE HEALTHCARE (Sept. 10, 2019, 11:07AM), https://www.fiercehealthcare.com/tech/mayo-clinic-taps-google-cloud-as-strategic-partner-to-accelerate-innovation-ai-digital [https://perma.cc/9RMS-4E95].

[153] *See* Roberta Pastorino et al., *Benefits and Challenges of Big Data in Healthcare: An Overview of the European Initiatives*, 29 EUR. J. PUB. HEALTH 23, 24–25 (2019).

[154] Mark W. Friedberg et al., *Factors Affecting Physician Professional Satisfaction and Their Implications for Patient Care, Health Systems, and Health Policy*, 3 RAND HEALTH Q. (Winter 2014), at 2–6.

grade for usability based on physician responses.[155] By contrast, Google Search is considered an "A" and the gold standard for system usability.[156] Due to poor usability, physicians now spend more time on EHR-related activities than they spend face-to-face with patients.[157] In another study, researchers found that the sheer number of messages and notifications that come from EHR tools lead to burnout and the desire to reduce clinic hours.[158] Enter Big Tech. To increase usability, Google is developing Guardian, a patient medical record search tool which "looks much like the company's flagship search engine."[159] Guardian comes equipped with auto-fill suggestions and can show patient information like vital tests and surgical history in one click.[160] Voice assistants like Alexa are also viewed as a new way to lessen administrative burdens and combat physician burnout, as voice commands and oral documentation are less taxing than navigating EHR tools.[161]

---

[155] Edward R. Melnick et al., *The Association Between Perceived Electronic Health Record Usability and Professional Burnout Among US Physicians*, 95 MAYO CLINIC PROC. 476, 477, 485 (2020).

[156] *Id.* at 477 (noting that "Google . . . ranks in approximately the top 0.01% of technologies evaluated").

[157] *See id.* at 476; Ming Tai-Seale et al., *Electronic Health Record Logs Indicate That Physicians Split Time Evenly Between Seeing Patients and Desktop Medicine*, 36 HEALTH AFFAIRS 655, 655 (2017) ("Our results suggest that the physicians logged an average of 3.08 hours on office visits and 3.17 hours on desktop medicine each day.").

[158] *See* Ming Tai-Seale et al., *Physicians' Well-Being Linked to In-Basket Messages Generated by Algorithms in Electronic Health Records*, 38 HEALTH AFFAIRS 1073, 1076 (2019).

[159] Copeland et al., *supra* note 3.

[160] *Id.*

[161] *See* Heather Landi, *NHS partners with Amazon to provide health information through Alexa*, FIERCE HEALTHCARE (July 11, 2019, 3:20 PM), https://www.fiercehealthcare.com/tech/nhs-partners-amazon-to-provide-health-information-through-alexa [https://perma.cc/UM2K-R36K]; *see also* Landi, *supra* note 35, at 1–2 (providing an overview on how Alexa and other voice command technology is being rolled out into the medical field).

[40] Finally, a data-driven approach can help improve overall healthcare experiences for patients. Networked systems and Big Data have revolutionized most industries, often leading to more user-friendly, personalized services for consumers. Some believe that this revolution has yet to reach the healthcare industry, and compared to other services, patients have become increasingly frustrated. Christopher Ross, Mayo Clinic's Chief Information Officer, argued that patients expect "the same experience as when they book an airline trip. They are looking for convenience, speed, immediacy, availability and high touch."[162] Medical-tracking apps, voice assistants, wearables, telemedicine and other new health tech are examples of ways that the medical industry may be brought into the Big Data paradigm and improve user experience.

2. Healthcare's Unique Moral Force

[41] Big Tech's disruption of healthcare follows a blueprint premised on a now-familiar bargain. Firms offer a service, often at no cost, in exchange for user data. The data is then used as a raw material to better personalize the service for the individual, while also predicting and influencing user behavior.[163] Search engines, "smart" technology, and mobile apps are all predicated on this exchange. Users often sacrifice privacy and autonomy as part of the bargain, as companies unilaterally set data collection conditions determining what data is collected, and ultimately, how it is used.[164] The healthcare revolution might be seen as a natural extension of these tried-and-true information business practices, and thus not deserving of any heightened consideration. But as the above examples indicate, while the digital healthcare revolution shares some similarities with data-driven innovations in other industries, its potential benefits—and ramifications—are unique. Put differently, healthcare is distinct, but its exceptionalism cuts in both directions. Healthcare regularly implicates life and death, pain and

[162] Landi, *supra* note 152.

[163] *See* ZUBOFF, *supra* note 66, at 93–94.

[164] *See generally id.* at 11 (explaining how AI can predict what you currently know, what you will know in the future, and how it all fits together).

suffering, and loss and grief. The benefits of improved and efficient care are different in kind than those felt in other industries impacted by Big Tech. Conversely, health information is often extremely personal and sensitive, and thus the most guarded category of data in the U.S. legal regime.[165] The stakes are high, and some believe that the potential damage from privacy harms, exploitation, and algorithmic bias are too great[166]. Yet a growing number of healthcare professionals argue that the promise of data-driven medical insights is too great, and patients should have a heightened obligation to cede their health information.[167] Ruth Faden et al. put this contention bluntly:

[42] "Traditional codes, declarations, and government reports in research ethics and clinical ethics have never emphasized obligations of patients to contribute to knowledge as research subjects. These traditional presumptions need to change. Just as health professionals and organizations have an obligation to learn, patients have an obligation to contribute to, participate in, and otherwise facilitate learning."[168]

[43] Faden et al. suggest a common purpose framework similar to that of John Rawls' common good principle.[169] "The common interest of members

[165] *See generally* HIPAA, 110 Stat. 1936 (providing the full HIPAA bill which encompasses the values of safeguarding personal medical information).

[166] *See, e.g.*, Katherine J. Igoe, *Algorithmic Bias in Health Care Exacerbates Social Inequities — How to Prevent It*, HARV. T.H. CHAN (Mar. 12, 2021), https://www.hsph.harvard.edu/ecpe/how-to-prevent-algorithmic-bias-in-health-care/ [https://perma.cc/SPP8-B3NZ].

[167] *See* Ruth R. Faden et al., *An Ethics Framework for a Learning Health Care System: A Departure from Traditional Research Ethics and Clinical Ethics*, 43 HASTINGS CTR. REP. 16, 23 (2013).

[168] *Id.*

[169] *Id.* (explaining that the framework is also grounded in the Humean concept of reciprocal obligation); JOHN RAWLS, A THEORY OF JUSTICE 205 (Harvard Univ. Press rev. ed. 1999) ("Government is assumed to aim at the common good, that is, at maintaining conditions and achieving objectives that are similarly to everyone's advantage.").

of a society in the healthcare system is that it be positioned to provide each person in the society with quality healthcare at a cost compatible with individual and societal economic well-being."[170] Under this framework, patient participation, through sharing data or otherwise participating in a so-called learning healthcare system, is necessary both to improve health outcomes and reduce health inequity.[171] Neither taxes nor fees can serve as substitutes for direct participation, and near universal participation is required to reap the collective benefits.[172] Faden et al. argue that the framework would still respect patient dignity by disclosing the ways in which data is used and how patient contributions have improved the healthcare system.[173] But dignity must also be viewed in light of the fact "the underprotection of patients from unjustified and often preventable harms and burdens in clinical practice is a profoundly serious moral problem."[174]

[44] In short, the increased collection of medical data is necessary to save lives. Under this framework, patient dignity, autonomy, and privacy are subordinated, and become a second-order consideration to the public good. The argument, while a departure from the status quo, demands to be taken seriously.[175] This line of thinking is also convenient for Big Tech, which is eager to justify its foray into healthcare as a way to better the world, not to advertise or collect user information. David Feinberg, head of Google

[170] Faden et al., *supra* note 167, at 23.

[171] *See id.*

[172] *Id.*; *see* Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 1, 11–13 (2000).

[173] Faden et al., *supra* note 167, at 25.

[174] *Id.* at 24.

[175] *See* discussion *infra* Section V (discussing how the U.S. health system is often criticized for over-prioritizing patient autonomy and privacy over broader principles of public good).

Health, says he came to Google "to make people healthy," not to "sell them ads."[176] Tim Cook believes his company's new healthcare focus will be Apple's greatest contribution to mankind.[177] Tech companies often categorize their health initiatives as altruistic ways to "help" the user, conveniently omitting how the companies stand to gain.[178] It is hard to take these claims at face value when the business models of the companies revolve around collecting data and selling targeted advertisements to individuals, especially considering that health data may be more valuable than most other types.[179] Moreover, talk of making the world a better place is reminiscent of self-serving phrases and mottos used by tech companies to validate extractive business practices.[180] Some companies, like Apple, have vowed to take medical privacy seriously, and not sell health data to

[176] Copeland et al., *supra* note 3.

[177] Gurdus, *supra* note 1.

[178] *See, e.g.*, *Connecting People With Health Resources*, FACEBOOK, https://preventivehealth.facebook.com/ [https://perma.cc/6MTF-NG9C]) ("Tens of millions of people in the US are missing out on recommended preventative care . . . . To help, we're working with US health organizations to offer a new Preventive Health tool . . . ."); *Live Your Healthiest Life*, GOOGLE HEALTH, https://health.google/#about [https://perma.cc/6U5N-A59F] ("Google Health is committed to helping everyone live more life every day through products and services that connect and bring meaning to health information.").

[179] *See, e.g.*, Will Maddox, *Why Medical Data is 50 Times More Valuable Than a Credit Card*, D MAGAZINE (Oct. 15, 2019, 11:09 PM), https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/ [https://perma.cc/L6D3-YLLD]; *From Big Data*, MASHABLE (Apr. 26, 2014), https://mashable.com/archive/big-data-pregnancy [https://perma.cc/3N6C-TGLG] ("According to Vertesi, the average person's marketing data is worth 10 cents; a pregnant woman's data skyrockets to $1.50.").

[180] *See* Honan, *supra* note 12.

advertisers.[181] But focusing on monetization alone misses another foundational aspect of data economies: tech companies benefit from health data collection whether they sell it or not. For example, when customers purchase an Apple Watch to track their steps and heartrate, the collected data becomes a raw input used to train and improve algorithms. The more data collected, the more opportunities to train the algorithm and better the product,[182] not to mention the valuable insights that can be gleaned by viewing data in the aggregate.[183] This is no different from the way that Google Search results become more accurate with every search ran.[184] Thus, data bounties in the healthcare industry mirror those in other informational-capitalist economies. Should the moral healthcare arguments extend to Big Tech practices despite the economic rewards these companies stand to gain? If so, what types of data collection should be permitted under this framework? And how does it account for other values implicated, like exploitation and equity?

[45] Faden et al. categorize different levels of patient obligation.[185] Participation in a randomized clinical trial, for instance, would not be required.[186] But other activities, like providing deidentified medical records, would be obligatory if they possessed a reasonable likelihood of improving healthcare quality.[187] The distinction between these two practices comes

[181] *Protecting User Privacy*, APPLE INC., https://developer.apple.com/documentation/healthkit/protecting_user_privacy [https://perma.cc/K7BN-A4Z9] ("Your app may not use information gained through the use of the HealthKit framework for advertising or similar services. . . . You can't sell information gained through HealthKit to advertising platforms, data brokers, or information resellers."); *see* NPR: ALL TECH CONSIDERED, *supra* note 65.

[182] *See* ZUBOFF, *supra* note 66, at 69–70.

[183] *See id.*

[184] *Id.*

[185] Faden et al., *supra* note at 167, at 23.

[186] *Id.*

[187] *Id.*

from their relative impacts on patient dignity, the risks and burdens they impose on patients, and the contrast in public and private health benefits.[188] While this framework may have theoretical appeal, it quickly breaks down when applied to messy Big Tech practices.

[46] Where do questions of moral obligation, dignity, and disclosure fit into a quickly evolving and expanding digital health landscape? It is unlikely that the framework would require someone to buy wearables like a Fitbit or Apple Watch. But might it justify Facebook reading private messages to monitor suicide potential, or covertly trying to purchase deidentified medical records?[189] What about social and commercial data from which medical predictions can be inferred?[190] Will users be required to accept this data collection, even it if has non-healthcare benefits? While medical innovation may promise to save lives and provide better quality of life, the moral force behind such a justification is tricky to apply, given the myriad ways medical information can now be obtained. Moreover, the pace of innovation makes delineating between permissible and prohibited types of medical collection difficult. By the time ethical consensus is built, the practice may already be obsolete.

[47] At the moment, these kinds of discussions are largely irrelevant due to lack of oversight, both internally and externally. Though similar discussions may take place in these companies' ethics departments, they may be fraught with recent attempts to reconcile corporate motivations with a heightened focus on racial and economic justice.[191] Rather, the discussion helps illustrate that moral arguments made by healthcare practitioners

[188] *See id.* at 25.

[189] *See* Fazzini & Farr, *supra* note 70.

[190] *See* Figueroa, *supra* note 84.

[191] *See* Rachel Sandler, *Head of Google Ethical AI Team Fired Three Months After Co-Leader's Controversial Exit*, FORBES (Feb. 19, 2021, 8:26 PM), https://www.forbes.com/sites/rachelsandler/2021/02/19/head-of-google-ethical-ai-team-fired-three-months-after-co-leaders-controversial-exit/?sh=46b57b1e3bb3 [https://perma.cc/4JSG-BD5T].

should be taken seriously, but similar arguments made by Big Tech are messy, and largely rhetorical.

IV. HARMS AND GAPS IN THE NEW PARADIGM

[48] Data-driven medical technologies offer immense potential to improve treatment and save lives. But with these new tools also comes an array of harms and opportunities for misuse. Many of these harms stem from breaches of patient and user privacy. Medical data hacks are already frequent given the enormous value of health data.[192] Beyond breaches, users suffer when they do not fully understand how, with whom, and for what purpose their medical information is shared. In addition to privacy harms, healthcare systems built on machine learning and algorithmic decision making are prone to bias and discrimination. Current legislation is not equipped to protect users and patients from these new harms. The data protection offered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is no longer robust, protecting only a limited number of entities and data, and leaving uncovered virtually every recent digital healthcare development.[193] Furthermore, even data protected under HIPAA is vulnerable to security breaches and reidentification.[194]

[49] While updated legislation and increased oversight are necessary, they will not be a panacea. Rather, tradeoffs and difficult choices are unavoidable. Privacy and public utility are often at odds: the more protections on data, the less researchers can learn from the data set. While new tracking and monitoring devices could save lives and improve

[192] *See* U.S. DEP'T OF HEALTH & HUM. SERVS. OFF. FOR CIVIL RTS., CASES CURRENTLY UNDER INVESTIGATION, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [https://perma.cc/4KWK-H9CU] (investigating breaches affecting HIPAA-covered entities with more than 500 individuals that occurred over past two years).

[193] *See generally* HIPAA, 110 Stat. 1936 (showing how HIPAA protects a limited number of entities and data which leaves uncovered virtually every recent digital healthcare development).

[194] See *infra* Section IV.A.2.C.

treatment, they may also exacerbate existing healthcare inequities. Section IV, offers a comprehensive framework for how legislation should begin to grapple with these issues. The following Section sketches the profound legislative gaps that have emerged from the digital healthcare revolution, and the harms that follow.

A. Privacy Harms and HIPAA's Waning Relevance

1. Privacy Harms in the Digital Health Paradigm

[50] New streams of health data provide new opportunities for encroachments on patient and user privacy. Even in the nascent digital healthcare industry, privacy harms are common. Health apps frequently mislead users about their data sharing practices. A recent study found that over eighty percent of the top-ranked apps for depression and smoking cessation shared data with Google and Facebook for marketing purposes, though fewer than half of these apps disclosed the sharing to users.[195] Some apps had privacy policies, yet did not include information about the data sharing in the policy.[196] In another instance, the period-monitoring app Flo settled with the Federal Trade Commission (FTC) after misleading its 100 million users about data collection practices.[197] In its privacy policy, Flo told users that it collected data only to provide necessary services, but actually shared sensitive health data with Facebook and Google.[198] The information included users' history regarding menstrual cycle, pregnancy, and childbirth.[199] Flow did not restrict Facebook and Google's access to the

[195] Kit Huckvale et al., *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, JAMA NETWORK OPEN, Apr. 19, 2019, at 1.

[196] *Id.* at 4–5.

[197] Singer, *supra* note 13.

[198] *Id.*

[199] *Id.*

data, which allowed the companies to use the health information for advertising purposes.[200]

[51] Other harms stem from weak security practices, which lead to vulnerabilities and breaches. Due to the value of medical data, attackers constantly target the healthcare industry. From 2005- 2019, seventy-six percent of all data breaches occurred in the healthcare industry, affecting close to 250 million individuals.[201] In the new paradigm where health data collection is decentralized, breaches may become more common, as the owners of new health apps and health tech may not have the expertise to develop robust security mechanisms. For example, Glow, another popular fertility and menstrual cycle tracking app, paid $250,000 as part of a settlement with the state of California.[202] A vulnerability in the app allowed hackers access to intimate personal information, like users' history of abortion and sex drive.[203] Attackers could also gather email addresses, change passwords, and access community forum posts, making it "easy for stalkers, online bullies, or identity thieves to use the information they gathered to harm Glow's users."[204] Exploiting the vulnerability did not require sophisticated hacking skills.[205] In another case, a loophole on Facebook allowed third parties access to the names of people in private, closed Facebook groups.[206] One of these groups was a community for women with a mutated BRCA gene, a condition that makes breast cancer

[200] *Id.*

[201] Adil Hussain Seh et al., *Healthcare Data Breaches: Insights and Implications*, 8 HEALTHCARE 133, 135–37 (2020).

[202] Beilinson, *supra* note 13.

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] Fazzini & Farr, *supra* note 70.

more likely.[207] A Google Chrome extension allowed anyone to download the names, email addresses, and personal information of all 9000 group members.[208]

[52] These examples show practices endemic to the internet and networked societies. Information thought to be protected can be hacked and accessed at a moment's notice. The sensitivity inherent to medical information has given rise to healthcare exceptionalism, the idea that healthcare data should be among the most protected personal information in our society.[209] There is no better manifestation of healthcare exceptionalism in the U.S. than HIPAA.[210] Yet, as discussed below, the digital healthcare revolution has destabilized both HIPAA and the very notion of healthcare exceptionalism.

2. HIPAA and its Waning Relevance

[53] In the U.S., healthcare data privacy is governed primarily by HIPAA. Four years after HIPAA's enactment, the U.S. Department of Health and Human Services (HHS) promulgated the HIPAA Privacy Rule to create safeguards for protected health information (PHI), which includes most individually-identifiable health information.[211] Covered entities—which includes health plans, healthcare clearinghouses, healthcare providers who transmit health information electronically, and their business

[207] *BRCA: The Breast Cancer Gene*, NAT'L BREAST CANCER FOUND., INC. (Apr. 15, 2020), https://www.nationalbreastcancer.org/what-is-brca [https://perma.cc/K9GK-TL5V].

[208] Fazzini & Farr, *supra* note 70.

[209] Terry, *supra* note 148, at 169–70.

[210] *Id.* at 170.

[211] *See* 45 C.F.R. § 164.502(d) (2020).

associates—cannot use or disclose PHI except in limited circumstances.[212] Covered entities may only use PHI for research purposes if they obtain written patient authorization, or if such authorization is impractical, obtain a waiver from an institutional review board.[213] Patient authorization or a waiver is not required, however, for datasets deemed deidentified.[214] In fact, there are no restrictions on the use or disclosure of deidentified data.[215] Data sets may be deidentified in two ways. One approach, the expert determination method, requires a person with appropriate knowledge to determine that the risk of reidentifying an individual is very small.[216] The other, the safe harbor method, requires eighteen individual identifiers to be removed from the dataset.[217]

[54] HIPAA has been called a "high-water mark" of PHI protection.[218] When enacted, HIPAA was considered robust, and many thought it was overprotective and burdensome.[219] But current practices threaten to make the Act obsolete. Each foundation of HIPAA—its sectoral nature, its focus

[212] *Id.* §§ 160.102(b), 160.103, 164.502(a)(1); *see* Price & Cohen, *supra* note 2, at 39 ("HIPAA allows use of PHI for health care treatment (including 'quality improvement'), operations, payment, public health, and law enforcement . . . .").

[213] 45 C.F.R. § 164.512(i)(1)(i); Roberta B. Ness, *Influence of the HIPAA Privacy Rule on Health Research*, 298 JAMA 2164, 2164 (2007).

[214] *See* 45 C.F.R. § 164.514(a).

[215] U.S. DEP'T HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 4 (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/6DGT-5QSE].

[216] 45 C.F.R. § 164.514(b)(1)(i).

[217] *Id.* § 164.514 (b)(2) (listing identifiers including names; geographic subdivisions smaller than a state; dates relating to an individual like birth date or discharge date; telephone numbers; social security numbers; email addresses; biometric identifiers; and medical record numbers).

[218] Ohm, *supra* note 5, at 1737.

[219] *See* Price & Cohen, *supra* note 2, at 39.

on PHI, and its emphasis on deidentification—has been undermined by new technologies and data practices. As a result, virtually all the data collection practices described in this article fall outside of HIPAA's purview.

a. Sectoral Nature Leads to Gaps in Protection

[55] The first, and most glaring, of HIPAA's inadequacies is the Act's emphasis on covered entities. HIPAA's narrow focus on a limited number of covered healthcare providers, rather than the health data itself, leaves profound gaps in federal health privacy law. In the 20th-century paradigm, where practically all health information originated and flowed through traditional healthcare providers, the covered entities system was workable. But the severe, 21st-century disruption of healthcare by Big Data and Big Tech blurs lines and ultimately lands many of today's largest health data collectors outside of the HIPAA framework.[220] As detailed above, today's digital titans now track, collect, and infer vast amounts of medical information.[221] Yet none of these practices are covered by HIPAA. Wearable devices that collect core health data like blood pressure, heart rate, and oxygen levels, are not covered. Glow's lax security mechanisms may have violated California law, but the app itself is not covered by HIPAA. And though HIPAA protects test results showing a patient has the BCRA gene mutation, it has little to say about a Facebook group disclosing the same information.[222] As the number of new medical data sources grows, HIPAA stands to go from the rule to the exception with so much health information free for the taking.

[220] I. Glenn Cohen & Michelle M. Mello, *Big Data, Big Tech, and Protecting Patient Privacy*, 322 JAMA 1141, 1141–42 (2019) ("HIPAA is a 20th-century statute ill equipped to address 21st-century data practices.").

[221] *See supra* Section II.

[222] *See* Fazzini & Farr, *supra* note 70.

b. PHI as a Game of Whack-a-mole

[56] Another central characteristic of the HIPAA regime is the reliance on personal health information (PHI) as a way to guide the sharing of medical data. PHI was an attempt by Congress to strike a balance between patient privacy and medical research.[223] By identifying and scrubbing datasets of particularly sensitive personal information, researchers could still glean insights from deidentified information.[224] Unfortunately, data innovations have outmoded PHI-dependent privacy practices. HIPAA's list of eighteen PHI identifiers becomes increasingly outdated with each passing day. At the time of enactment, the list may have seemed robust. However, Congress "froze these conclusions in amber, enumerating a single, static list" of PHI that has gone largely unchanged.[225] Given the rate of change in the industry, any list of PHI would need constant revision. But even if HHS expanded its definition of PHI, the enterprise would turn into a futile game of "whack-a-mole."[226] Data analytics now allow medical information to be inferred from Facebook "Likes," Instagram filters, and Twitter posts.[227] PHI now springs from sources that were once unimaginable. Potential sources of PHI will only increase as the inferential power of Big Data becomes stronger.[228] If medical inferences can be drawn from religious language in social media posts, what *would not* qualify as

[223] *See* Ohm, *supra* note 5, at 1737.

[224] *See id.* at 1716.

[225] *Id.* at 1737.

[226] *Id.* at 1742; *see also* I. Glenn Cohen & Michelle M. Mello, *HIPAA and Protecting Health Information in the 21st Century*, 320 JAMA 231, 231–32 (2018) ("Another solution involves revisiting the list of identifiers to remove from a data set. There is no doubt that regulations should reflect up-to-date best practices in deidentification. However, it is questionable whether deidentification methods can outpace advances in reidentification techniques given the proliferation of data in settings not governed by HIPAA and the pace of computational innovation.").

[227] *See supra* Section II.B.2.

[228] *See* Ohm, *supra* note 5, at 1742 (describing PHI as an "ever-expanding category").

PHI?[229] Any attempt to modernize the list of PHI would need constant revision and inevitably become too large, thus swallowing the rule and defeating the purpose of having an exhaustive, finite list.

c. Misplaced Reliance on Deidentification

[57] Under HIPAA, PHI-scrubbing and deidentification work in tandem. Under the Act, data that is deidentified is no longer protected.[230] The idea was that data without PHI is "anonymous," and once that data becomes anonymous, it remains anonymous. As detailed above, the assumption that PHI-scrubbed data is anonymous has already broken down. The second assumption, that anonymous data will stay anonymous, has also been undermined by new data reidentification techniques.[231] Data thought to be anonymized may still contain unique identifiers that, when paired with other data sets, reveal information believed to be scrubbed.[232] The more information an outside adversary has, the easier it is to reidentify data.[233] The ubiquity of data sets from geographic, social, and commercial sources, paired with the surge of new healthcare information streams, only increase the risk of reidentification.[234] These developments lead to the uncomfortable realization that privacy and public utility are "two

[229] *See, e.g.*, Merchant et al., *supra* note 78, at 7 (finding that "the top 25% of patients mentioning the (god, family, pray) topic were 15 times . . . more likely to have been diagnosed with diabetes than those in the bottom 25% of mentioning that same topic").

[230] U.S. DEP'T HEALTH & HUMAN SERVS., *supra* note 215, at 4.

[231] *See* Ohm, *supra* note 5, at 1740 ("Easy reidentification makes PII-focused laws like HIPAA underprotective by exposing the arbitrariness of their intricate categorization and line drawing.").

[232] *See, e.g.*, *id.* at 1717–22; Latayna Sweeney, *Simple Demographics Often Identify People Uniquely* 1–2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000).

[233] Ohm, *supra* note 5, at 1740.

[234] *See* Letter from William W. Stead, Chair, Nat'l Comm. on Vital & Health Stat., to Thomas E. Price, Sec'y, Dep't Health & Hum Servs. (Feb. 23, 2017), https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf [https://perma.cc/9CUH-RYA5].

fundamentally conflicting requirements."[235] "Data can be either useful or perfectly anonymous but never both . . . no regulation can increase data privacy without also decreasing data utility. No useful database can ever be perfectly anonymous, and as the utility of data increases, the privacy decreases."[236] Further, the inverse relationship between privacy and utility is skewed: small increases in utility beget larger decreases in privacy, and small increases in privacy cause larger decreases in utility.[237] As a result, in order to realize the potential public benefits of new healthcare information technologies, some level of privacy must be compromised. Thus, while it is important to acknowledge the current health-privacy framework is unequipped to handle emerging practices, it is also necessary to accept that tradeoffs are unavoidable. The common purpose framework must be viewed in light of these new understandings. New learning capabilities will inevitably jeopardize patient and user privacy, encroaching on the concerns the framework purports to protect.

B. Inferences, Judgments, Research, and Bias

[58] The new digital healthcare paradigm relies on prediction and inference to reach algorithmic judgments. While inference-backed decision making can lead to a more effective healthcare system, algorithmic judgments also risk reproducing and exacerbating inequalities. In medical contexts, two practices are particularly worrisome: algorithmic decision making based on biased or unrepresentative data, and discrimination against inferred, protected medical traits.

---

[235] Shuchi Chawla et al., *Toward Privacy in Public Databases*, *in* THEORY OF CRYPTOGRAPHY 363, 363–64 (Joe Kilian ed. 2005).

[236] *See* Ohm, *supra* note 5, at 1704–06.

[237] *Id.* at 1755; *see* Justin Brickell & Vitaly Shmatikov, *The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing*, ASS'N FOR COMPUTING MACH. (14th ACM Int'l Conf. on Info. & Knowledge Mgmt., Las Vegas, Nev.), Aug. 24, 2008, at 70 ("[E]ven modest privacy gains require almost complete destruction of the data-mining utility.").

1. Algorithmic Medical Judgments and Their Shortcomings

[59] Much of data's value comes from its inferential power.[238] From inferences, judgments and decisions are made about users and patients. Inference-based medical judgments are concerning, as they are often unverifiable and inaccurate.[239] While some of these decisions are benign—like which shoe to advertise to consumers—a growing number of judgments are more consequential.[240] The new digital healthcare paradigm ushers in a new wave of inferences and judgments. Some of these decisions, like medical diagnoses, can be matters of life and death. Despite the stakes, clinical algorithms have already shown bias, and are often disproportionately more effective for some groups than others.[241] The threat of unequal diagnosis and treatment is only heightened by new medical technologies developed outside of the traditional, regulated healthcare industry.

[60] In medical algorithmic contexts, training data bias is common. There are two distinct types of training data bias. First, the algorithm "treats cases in which prejudice has played some role as valid examples to learn from" and reproduces the bias.[242] Second, the algorithm learns from "a

[238] *See supra* Section II.B.2.

[239] *See* Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2 COLUM. BUS. L. REV. 494, 497 (2019).

[240] *See id.* at 506–07 ("Numerous applications of Big Data analytics to draw potentially troubling inferences about individuals and groups have emerged in recent years. Major internet platforms are behind many of the highest profile examples: Facebook may be able to infer sexual orientation—via online behavior or based on friends—and other protected attributes (e.g., race), political opinions and sadness and anxiety – all of these inferences are used for targeted advertising.").

[241] *See, e.g.*, Obermeyer et al., *supra* note 15, at 366; Alicia R. Martin et al., *Clinical Use of Current Polygenic Risk Scores May Exacerbate Heath Disparities*, 51 NATURE GENETICS 584, 584 (2019).

[242] Barocas & Selbst, *supra* note 4, at 681.

biased sample of the population" which may "systematically disadvantage those who are under- or overrepresented in the dataset."[243] While both are forms of prejudice, algorithmic bias is frequently subtle, unintentional, and difficult to detect. Often, the bias stems from reproduction of past inequities based on race, gender, or income. Training bias problems are difficult to detect because developers rarely disclose data used for training algorithmic systems.[244]

[61] Data-driven healthcare tools already exhibit training bias. Polygenic risk scores, a new precision medicine tool, use genome-wide association studies to predict risk of disease.[245] While the risk scores show promise, they have thus far been disproportionately more effective for patients of European ancestry than those of other backgrounds.[246] This is because efforts in genome discovery have relied heavily on participants from European descent.[247] Worse, non-European participation in genome-wide association studies has declined or stagnated since 2014.[248] Use of polygenic risk scores in their current state risk exacerbating inequities in healthcare systems. In another instance, a healthcare algorithm severely underestimated health risks for Black patients in comparison to white patients.[249] The algorithm used past health costs as a proxy to predict future

[243] *Id.*

[244] David Danks & Alex John London, *Algorithmic Bias in Autonomous Systems*, AAAI PRESS (26th Int'l Joint Conf. on A.I., Melbourne, Austl.), Aug. 19–25, 2017, at 4691, 4692.

[245] *See* Martin et al., *supra* note 241, at 584.

[246] *Id.*

[247] *Id.* (explaining that while those of European descent account for 16 percent of the global population, they comprise roughly 79 percent of all genome-wide association study participants.)

[248] *Id.*

[249] Obermeyer et al., *supra* note 15, at 366.

healthcare needs.[250] As Black patients have historically received, and still receive, less healthcare than white patients, the training data was distorted, and the algorithm reproduced past inequities.[251] While the study focused on a specific algorithm, "the same issue almost certainly exists in other tools used by other private companies, nonprofit health systems and government agencies to manage the healthcare of about 200 million people in the United States each year."[252]

[62] Past regulation anticipated that research and development for medical would occur in universities or as part of health systems.[253] Yet, the above examples show that algorithmic inequities exist in medical industries despite such regulation.[254] New commercial healthcare algorithmic devices fall outside of any scrutiny, which exacerbates the potential for bias and inequitable design.[255] It is not difficult to imagine how training data biases could manifest in Big Tech health tools. Monitoring and tracking devices are expensive and may only be available to certain, more affluent populations. If devices are trained on this data alone, their diagnostic power may be less effective for marginalized groups. For example, in the Apple-

[250] *See* Cohen & Mello, *supra* note 226, at 1141.

[251] Obermeyer et al., *supra* note 15.

[252] Carolyn Y. Johnson, *Racial bias in a medical algorithm favors white patients over sicker black patients*, WASH. POST (Oct. 24, 2019), https://www.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients/ [https://perma.cc/PP2F-YAPL].

[253] Cohen & Mello, *supra* note 226, at 231.

[254] *See generally* 45 C.F.R. § 46.101 (2019) (explaining the regulations put in place to protect human subjects when conducting research).

[255] *See* U.S. FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES (2019) (explaining that while certain medical devices and medical software are regulated by the Food and Drug Administration (FDA), many are not and the 21st Century Cares Act recently amended the definition of medical devices under Federal Food, Drug, and Cosmetic Act to exclude many digital health devices); Timo Minssen et al., *Regulatory Responses to Medical Machine Learning*, 7 J.L. & BIOSCIENCES 1, 2, 4, 16–17 (2020).

Stanford irregular heartbeat study, white males aged 22–39 were overrepresented.[256] The percentage of Black participants was roughly half of the national Black population percentage.[257] The Hispanic population was even less representative of the national average.[258] The study also did not account for patient income level or access to healthcare. These problems may only worsen if users rely on Big Tech tools instead of more regular medical checkups, or if hospitals incorporate new technologies that rely on data collected and trained without scrutiny.

[63] Lack of both internal and governmental oversight in Big Tech is even more worrisome, given companies' penchants for experimenting on uninformed test subjects.[259] To study what drives emotional expression on its platform, Facebook manipulated users' news feeds to show expressive content.[260] Facebook did not inform the selected users about the study, instead arguing that its blanket data policy constituted informed consent.[261] Facebook also conducted political experiments that evaluated how "get out the vote" messages affected users' willingness to vote.[262] The studies made no mention of user notice or consent. New streams of medical data enhance Big Tech's experimentation power and raise the stakes. Without proper oversight, training and experimentation could have life-and-death

[256] *See* Perez et al., *supra* note 116, at 1914.

[257] *Id.*; *Quick Facts: United States*, U.S. CENSUS BUREAU (July 1, 2019), https://www.census.gov/quickfacts/fact/table/US/PST045219 [https://perma.cc/D98L-L6GS].

[258] Perez et al., *supra* note 116, at 1914; *see* U.S. CENSUS BUREAU, *supra* note 257.

[259] See, e.g., Perez et al., *supra* note 116, at 1914.

[260] Adam D. I. Kramer et al., *Experimental Evidence of Massive-scale Emotional Contagion Through Social Networks* 111 PNAS 8788, 8788 (2014).

[261] *Id.* at 8789.

[262] Jason J. Jones et al., *Social Influence and Political Mobilization: Further Evidence from a Randomized Experiment in the 2012 U.S. Presidential Election*, PLOS ONE, Apr. 26, 2017, at 1–2; Robert M. Bond et al., *A 61-Million-Person Experiment in Social Influence and Political Mobilization*, 489 NATURE 295, 295 (2012).

consequences. It cannot be forgotten that medical research oversight came after the exploitative and racist methods used in the Tuskegee Study.[263]

[64] An equally important lesson from the Tuskegee Study is that human judgment is not free of bias either, particularly in medical contexts. Still today, white laypeople and medical students hold false beliefs about biological differences between Black and white persons, leading to racial bias in pain perception and treatment recommendation accuracy.[264] Race has also been associated with doctors' assessment of patient intelligence, likelihood of risk behavior, and adherence with medical advice.[265] More worrisome, human bias is more difficult to fix than algorithmic bias.[266] Furthermore, commonplace, non-data-driven medical technologies, like oximeters, have exhibited bias for decades.[267] In fact, many welcome

[263] *See* Eli Y. Adashi et al., *The Belmont Report at 40: Reckoning with Time*, 108 AM. J. PUB. HEALTH 1345, 1345 (2018) ("[T]he Tuskegee Syphilis Study made it plain that the moral foundation of human subject research was in desperate need of repair. . . It was against this backdrop that Congress resolved to act. Numerous hearings and multiple spirited discussions later, an agreement was struck to constitute the 'Commission.' The outgrowth of a retreat held at the Smithsonian Institution's Belmont Conference Center, the *Belmont Report* lays out a principled analytical frame-work to 'guide the resolution of ethical problems arising from research involving human subjects.'").

[264] *See* Kelly M. Hoffman et al., *Racial Bias in Pain Assessment and Treatment Recommendations, and False Beliefs About Biological Differences Between Blacks and Whites*, 113 PNAS 4296, 4296 (2016).

[265] Michelle van Ryn & Jane Burke, *The Effect of Patient Race & Socio-economic Status on Physicians' Perceptions of Patients* 50 SOC. SCI. & MED. 813, 813 (2000).

[266] Sendhil Mullainathan, *Biased Algorithms Are Easier to Fix Than Biased People*, N.Y. TIMES (Dec. 6, 2019), https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html [https://perma.cc/JA6L-LATS] ("Changing people's hearts and minds is no simple matter. . . . Changing algorithms is easier than changing people: software on computers can be updated; the 'wetware' in our brains has so far proven much less pliable.").

[267] *See, e.g.*, Michael W. Sjoding et al., *Racial Bias in Pulse Oximetry Measurement*, 383 NEW ENG. J. MED. 2477, 2477 (2020); John Feiner et al., *Dark Skin Decreases the Accuracy of Pulse Oximeters at Low Oxygen Saturation: The Effects of Oximeter Probe Type and Gender*, 105 ANESTHESIA & ANALGESIA 18, 22 (2007).

medical AI and machine learning tools ass opportunities to root out existing human biases.[268] These examples do not suggest that new algorithmic devices are an immediate upgrade on the status quo. Rather, they serve as a reminder that any analysis of the new digital healthcare regime must answer the baseline question, "compared to what?"

2. Inference-Backed Medical Discrimination

[65] A similar concern to algorithmic bias comes from discrimination rooted in inferences of protected medical traits. Data brokers have long been able to infer protected characteristics like race,[269] sexual orientation,[270] and age.[271] Now, protected medical characteristics can also be inferred, thanks to new streams of healthcare information and improved data analytics.[272]

[66] Existing legislation may prevent some medical-inference discrimination. For example, in 2019, Facebook settled with the Department of Housing and Urban Development (HUD) for violating the Fair Housing

---

[268] Milena A. Gianfrancesco et al., *Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data*, 178 JAMA INTERNAL MED. 1544, 1545 (2018) ("A promise of machine [sic] learningin health care is the avoidance of biases in diagnosis and treatment. Practitioners can have bias in their diagnostic or therapeutic decision [sic] makingthat might be circumvented if a computer algorithm could objectively synthesize and interpret the data in the medical record and offer clinical decision support [sic] toaid or guide diagnosis and treatment.").

[269] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 19–20 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/LAG3-28D2].

[270] *See, e.g.*, José González Cabañas et. al., *Facebook Use of Sensitive Data for Advertising in Europe*, ARXIV (2018) at 1, 1–2.

[271] Jinxue Zhang et. al., *Your Age Is No Secret: Inferring Microbloggers' Ages Via Content and Interaction Analysis*, AAAI PRESS (10th Int'l AAAI Conf. on Web and Soc. Media, Cologne, Ger.), May 17–20, 2016, at 476–77.

[272] *See supra* Section II.B.1.

Act. [273] "Facebook didn't show ads to people who listed things like 'child care,' 'mobility scooters,' or 'assistance dog' as interests."[274] HUD enjoined the discriminatory practices, forcing Facebook to reconsider its microtargeting advertising campaign.[275] Enforcement of anti-discrimination statutes has also forced Facebook to retool its job and loan advertising system,[276] and a similar complaint was filed against Facebook for allowing sex discrimination in hiring practices, violating Title VII.[277] Still, some anti-discrimination statutes are ill-suited for digitized discrimination. While Title III of the Americans with Disability Act, which prohibits disability-based discrimination in places of public accommodation, might theoretically cover social media platforms, courts have not provided a clear answer.[278]

---

[273] Housing Charge of Discrimination, Assistant Sec'y for Fair Hous. & Equal Opportunity v. Facebook, Inc., FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf [https://perma.cc/N4PY-AU9E].

[274] Andrew Liptak, *The US government alleges Facebook enabled housing ad discrimination*, VERGE (Aug 19, 2018, 5:36 PM), https://www.theverge.com/2018/8/19/17757108/us-department-of-housing-and-urban-development-facebook-complaint-race-gender-discrimination [https://perma.cc/M3UD-A6U9].

[275] *See id.*

[276] Tracy Jan & Elizabeth Dwoskin, *Facebook Agrees to Overhaul Targeted Advertising System for Job, Housing and Loan Ads After Discrimination Complaints*, WASH. POST (Mar. 19, 2019), https://www.washingtonpost.com/business/economy/facebook-agrees-to-dismantle-targeted-advertising-system-for-job-housing-and-loan-ads-after-discrimination-complaints/2019/03/19/7dc9b5fa-4983-11e9-b79a-961983b7e0cd_story.html [https://perma.cc/XR58-B67F].

[277] Galen Sherwin, *How Facebook Is Giving Sex Discrimination in Employment Ads a New Life*, Am. Civ. Liberties Union. (Sep. 18, 2018, 10:00 AM), https://www.aclu.org/blog/womens-rights/womens-rights-workplace/how-facebook-giving-sex-discrimination-employment-ads-new [https://perma.cc/GRJ4-FSPB].

[278] Mason Marks, *Algorithmic Disability Discrimination*, *in* DISABILITY, HEALTH, LAW AND BIOETHICS 245, 245 (I. Glenn Cohen et al. eds., 2020).

[67] These forms of overt inference-based discrimination are relatively straightforward to detect and remedy. Unfortunately, the Big Data paradigm presents unintentional discrimination that is much harder to detect. Inferences and causal connections are the backbone of targeted advertising and internet personalization. They can also lead to microtargeting and behavioral nudges which are discriminatory in nature. A classic example comes from Latanya Sweeney's seminal research on Google ads. Sweeney found that Google search results for names more often associated with Black individuals, like Latanya or Latisha, more often displayed ads incorporating those names with arrest records than names associated with white individuals, like Kristen or Jill.[279] In another example, Google search's autofill function suggested completing the phrase "transgenders are" with words like "freaks," "gross," and "sick."[280] In both instances, Google's algorithm learned from, and reproduced, users' preexisting biases.

[68] Similar practices could occur in medical contexts. Imagine an algorithm that can infer that an individual uses a wheelchair. The algorithm also knows that, for whatever reason, few users who use wheelchairs have engaged with a particular advertisement for a job listing. The algorithm therefore decides not to show the user the job listing. Replicated at scale, individuals who use wheelchairs disproportionately would receive fewer opportunities to search and find employment. Similar scenarios can be conceived in housing and education contexts, affecting anyone with perceived adverse medical conditions. This problem is only exacerbated by the fact that proprietary algorithms are protected by trade secret law, creating transparency issues.[281]

---

[279] Latanya Sweeney, *Discrimination in Online Ad Delivery*, 11 ACM QUEUE 1, 3–4 (2013).

[280] Jeremy Kun, *Big data algorithms can discriminate, and it's not clear what to do about it*, CONVERSATION (Aug. 13, 2015, 1:56 AM), https://theconversation.com/big-data-algorithms-can-discriminate-and-its-not-clear-what-to-do-about-it-45849 [https://perma.cc/27JA-NRPC].

[281] *See* Sonia K. Katyal, *Private Accountability in the Age of AI*, 66 UCLA L. REV. 54, 118, 120 (2019).

V. RESPONDING TO THE DIGITAL HEALTH REVOLUTION

[69] The ongoing transformation in the healthcare industry implicates values that strike to the core of human nature, like dignity, autonomy, equity, and fairness. It asks us to weigh these values against the backdrop of life and death, and requires the reconsideration of how data and personal information are protected. The revolution has also made many healthcare protections obsolete. This Section offers a framework to guide regulation that considers the values implicated by the digital health technologies and practices, suggesting a number of legislative requirements necessary for any regulation to adequately respond to the digital health revolution.

A. The Values Implicated by the Digital Health Revolution and How to Think Through Them

[70] To sufficiently respond the data-driven transformation of healthcare industries, any proposed legislation must account for all of the many competing considerations at stake. The following subsections discuss four core concerns that are implicated by the digital health revolution. These considerations stem from preexisting debates that this Article does not attempt to resolve. Rather, legislative answers should address these problems and attempt to strike a balance between competing concerns. Finally, although the presentation of these arguments is cost-benefit, the analysis is not strictly utilitarian in nature. Rather, any analysis should be pluralistic, accounting for egalitarian and dignitarian concerns.

1. Who Benefits?

[71] The first consideration asks, who benefits, and how are the benefits are distributed?[282] The question may seem straightforward, but in reality, it is highly nuanced and should be evaluated across different axes. First, is the

[282] *See* RONALD DWORKIN, SOVEREIGN VIRTUE: THE THEORY AND PRACTICE OF EQUALITY 428 (2000) ("We must ask, in considering whether any new technique should be permitted or regulated or forbidden, about the likely impact of any such decision on individual interests. Who will be better off and who worse off in virtue of any such decision?").

benefit primarily felt by private interests, or by the public? Second, within the public, do certain groups benefit more than others? Are benefits felt only by a select few? Do these benefits come at the expense of certain, vulnerable populations? While it is difficult to precisely quantify these benefits, a rough hierarchy may emerge. In this hierarchy, public, evenly-distributed benefits are presumptively favored and unevenly-distributed or private benefits are presumptively less favored.

a. Private and Public Good

[72] Digital health innovations have great potential to enhance public welfare. But tech firms are quick to justify exploitative tactics under the guise of the public benefit.[283] Policy should scrutinize new practices and technologies to determine true societal benefit. For instance, is user data collected for corporate profit, or is it aiding medical research? Does a data processer intend to sell collected medical data for targeted ads, or is collection solely for the user's benefit? Even amongst public health benefits, policy can delineate between certain goals and products. While tools designed to improve physician quality of life may be admirable and welfare-enhancing, their public benefits are more attenuated than machine learning tools used to detect and combat rare forms of cancer. Disentangling these benefits will not always be easy. Often, private and public gains will overlap. Partnerships with hospitals should not be disfavored simply because a corporate benefit exists, for without one we would not expect companies to pursue the agreements in the first place. Still, if a given technology or practice has overwhelmingly private or public benefits, such a determination can help guide regulation.

[73] Regulation can also evaluate private benefit at an industry or company-specific level, accounting for relative trustworthiness based on reputation and past practices.[284] For example, many period-tracking apps

[283] *See supra* Section III.

[284] *See* Ohm, *supra* note 5, at 1761 ("Do the history, practices, traditions, and structural features of the industry or sector instill particular confidence or doubt about the likelihood of privacy?").

have violated their privacy policies, sold advertising data to third parties, and instituted weak data security measures.[285] These inadequacies may lead regulators to implement heightened duties on all period tracking apps, at least temporarily. Similarly, a firm-by-firm assessment may lead regulators to think Facebook's healthcare data practices deserve heighted scrutiny, given its history of discriminatory advertising, security breaches, penchant for experimentation, and other privacy related issues. This trust-informed regulation serves two purposes. Most obviously, it increases protection where harm is most likely to occur. The secondary function is soft pressure on companies and industries with bad track records to improve their practices. However, regulating at a company-specific level will be burdensome, and such regulation should perhaps be reserved for particularly trustworthy or untrustworthy companies, or companies that are particularly active or that dominate a given sector of the digital health economy.

[74] Finally, policy should scrutinize the enclosure of biomedical commons by private technology firms.[286] Recent developments have led to a "corporate commons," particularly in biotechnology fields, where businesses co-opt community-held resources for their own private gain, and later restrict access to the information.[287] A parallel trend exists in consumer digital economies, where firms routinely enclose sections of the biopolitical public domain for their benefit, excluding others.[288] In health contexts, data collection should be viewed as a means to an end. The ultimate goal is the public health benefit received from the synthesis and analysis of the information. Thus, attempts to guard healthcare data for corporate interests, rather than individual privacy concerns, should be disfavored.

---

[285] *See supra* Section IV.A.1.

[286] *See* Donna Dickenson, *The Common Good*, *in* THE OXFORD HANDBOOK OF LAW, REGULALTION & TECHNOLOGY 135, 145–46 (Roger Brownsword et al. eds., 2017).

[287] *Id.* at 147–48.

[288] *See* Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213, 223–24 (2018).

b. Fairness and Distribution

[75] Even when health benefits are felt largely by the public, policy should still be mindful of how the benefits are distributed. Is it only affluent, historically advantaged populations who reap the rewards of these cutting-edge technologies, due to price or scarcity? Are certain algorithmic medical judgments routinely more accurate for some groups rather than others? If so, what is the appropriate response? Some argue we should level up rather than level down: if new health innovations provide tangible benefits, like increased life expectancy, potential for exacerbation of inequality should not prevent the use of these new technologies. For example, in a parallel debate surrounding genetic testing for disease prevention, Ronald Dworkin believed that genetic testing should not be prohibited solely because it is available to the rich.[289] Dworkin argued:

> It is true that the availability of such tests might further increase the advantages of the rich over the poor, either because the tests could be afforded only by the rich, or because the treatment that capitalizes on the information . . . is itself too expensive for some. But these disadvantages cannot outweigh the value of an increased life expectancy.[290]

[76] Dworkin warned against seeking equality by "leveling down," and believed that medical "techniques available for a time only to the very rich often produce discoveries of much more general value for everyone."[291] In similar healthcare debates, others have echoed Dworkin's sentiment that temporary inequities are justified if the benefits eventually trickle down to the rest of the public.[292] By contrast, an egalitarian approach might suggest

[289] DWORKIN, *supra* note 282, at 429.

[290] *Id.*

[291] *Id.* at 440.

[292] *See* Jeanne Snelling & John McMillan, *Equality: Old Debates, New Technologies*, *in* THE OXFORD HANDBOOK OF LAW, REGULATION & TECHNOLOGY 69, 84 (Roger Brownsword et al. eds., 2017).

that the risk of perpetuating already-existing social inequities is too great to adopt certain technologies.[293]

[77] Rather than attempt to resolve this debate, perhaps regulators could distinguish between technologies based on their short-term and long-term effects. New, expensive technologies that confer a health benefit only to affluent users might be unavoidable under any healthcare framework. Just as a rich patient could pay for an experimental cancer treatment, or eat an expensive, healthy diet, so too could they buy the most expensive Apple Watch with the most accurate ECG monitor.[294] We may worry less about this type of inequality, because these cutting-edge technologies will theoretically spread to a wider population. By contrast, egalitarian skepticism may be more appropriate when healthcare technologies internalize and learn from pre-existing inequalities, risking reproduction of these disparities. If the same, cutting-edge Apple Watch is used as part of a study on heart-irregularities, the pool of potential subjects would be unrepresentative of the general population, and thus concerns over fairness and bias would be heightened.

2. Autonomy, Paternalism, and Bargaining Power

[78] Data collection, prediction, and behavioral modification are foundational practices of the digital health regime. To what extent do these practices encroach on user autonomy, and should such encroachment be permissible? Do the public health benefits from loss of autonomy alter the analysis? These questions implicate a long-standing debate in the medical community. Autonomy is a foundational principle of bioethics and informs

[293] *Id.* at 85 ("[A] relational egalitarian would likely be concerned about the potential of genetic enhancement to build upon and perpetuate social inequality that exist because of past injustice and social structures that impact upon ethnic, gender, and cultural groups.").

[294] *See* DWORKIN, *supra* note 282, at 429.

other bedrock values such as privacy and consent.[295] But autonomy is not absolute, and in fact may be qualified by other competing concerns.[296] Some scholars argue that American bioethics overemphasizes autonomy, forcing patients to make burdensome choices. According to these critics, physicians should be more concerned about what patients should want rather than what they do want.[297] This orientation is much more paternalistic, and inevitably usurps autonomy.[298]

[79] This debate informs existing discussions about user autonomy in a digital setting. Today's tech titans offer services that personalize and predict, often in the name of convenience. A growing body of scholarship has criticized these practices for their reduction of individual autonomy.[299] Transposing this biomedical ethics debate to tech is relatively straightforward, though a few caveats are necessary. First, while tech firms increasingly act as medical providers, we would still hesitate to categorize their relationship with users as a traditional physician-patient relationship. Thus, we should not assume that autonomy standards in conventional healthcare settings will map perfectly onto the digital paradigm. We might think that the traditional healthcare settings require more attention to autonomy because in these settings, the stakes of decisions are higher. In doctor's offices, patients weigh the benefits of risky operations and engage in family planning. The consequences of these decisions have profound, long-term consequences on the patient, and thus the physician's influence over these decisions warrants heavy scrutiny. Currently, apps and digital health devices do not have direct influence over the same kinds of high-

[295] *See* TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 104 (8th ed. 2019) (respecting a patient's autonomy "is to acknowledge their right to hold views, to make choices, and to take actions based on their values and beliefs").

[296] *See id.*

[297] CARL E. SCHNEIDER, THE PRACTICE OF AUTONOMY: PATIENTS, DOCTORS, AND MEDICAL DECISIONS, at xi (1998).

[298] *See* BEAUCHAMP & CHILDRESS, *supra* note 295, at 104.

[299] ZUBOFF, *supra* note 66, at 11.

stakes medical decisions. Instead, these digital tools encroach on autonomy in much "softer" ways. As data-driven healthcare mechanisms become more commonplace, it is possible that users will make serious decisions over their phones instead of in the doctor's office. Ultimately, policy should look at both the importance of the decision, and the ways in which the decision can be influenced, to determine what level of autonomy users and patients should be given.

[80] Second, health predictions and nudges are different in-kind from those previously used in medical contexts. Google and Facebook are privy to troves of non-medical personal information. This might allow for more targeted nudging, which may be more intrusive but could also be more beneficial. For example, to steer smokers to quit, medical providers and government might employ an array of nudges. Governments could implement a sin tax[300] or require graphic images depicting the dangers of smoking on every cigarette packet.[301] Physicians could explain the risks of smoking to known smokers. These interventions, while beneficial, target smokers as a class, and are less intrusive. By contrast, tech companies could leverage their many data streams to make more individualized interventions. They may know when a given individual is most likely to smoke and intervene when the individual is most vulnerable.[302] Whether

[300] Aurelio Miracolo et al., *Sin Taxes and Their Effect on Consumption, Revenue Generation and Health Improvement: A Systematic Literature Review in Latin America*, 36 HEALTH & POL'Y PLAN., June 2021, at 709 ("Sin or public health taxes are excise taxes imposed on the consumption of potentially harmful goods for health").

[301] *See, e.g.*, Scott D. Halpern et al., *Randomized Trial of Four Financial-Incentive Programs for Smoking Cessation*, 372 NEW ENG. J. MED. 2108, 2108 (2015).

[302] *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1033 (2014) ("A given consumer may not be vulnerable most of the time and will act rationally in her own interest. But under very specific conditions—say, when confronted with scarcity by a trusted source after a long day at work or upon making her hundredth decision of a day—she may prove vulnerable for a short window. Therefore, a firm with the capacity and incentive to exploit a consumer could, for instance, monitor the number of decisions she makes on her phone and target the customer most intensely at the moment she is most depleted.").

such an intervention is impermissible, despite its beneficial outcomes, will depend on views on autonomy and paternalism.

[81] Of course, just as companies could nudge vulnerable users to make healthy decisions, they could just as easily nudge users to make unhealthy decisions that increase the companies' bottom lines.[303] And unlike doctors and physicians, tech firms are not bound to fiduciary duties with their users. While a growing number of academics have called for imposing a fiduciary duty between Big Tech companies and consumers,[304] and a recent legislative proposal would impose duties of care, loyalty, and confidentiality on online service providers,[305] there are inherent tensions within the digital information fiduciary framework that do not exist in the typical doctor-patient framework. Most notably, these companies have a fiduciary duty to shareholders.[306] If shareholder fiduciary duties require companies to maximize profits, it's difficult to imagine how a duty to users could coincide.[307] Furthermore, a digital fiduciary obligation would practically require entirely reimagining surveillance capitalist business practices. Companies like Facebook and Google, collect user information to understand and exploit users' vulnerabilities for profit. If targeted

[303] *See id.* ("[T]he concern is that hyper-rational actors armed with the ability to design most elements of the transaction will approach the consumer of the future *at the precise time* and *in the exact way* that tends to guarantee a moment of (profitable) irrationality.").

[304] *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1221 (2016) ("I do not claim that Facebook or Uber is managing my estate, or is my accountant, my doctor, or my lawyer. What I do claim is that in the digital age, because we trust them with sensitive information, certain types of online service providers take on fiduciary responsibilities."); *Ohm*, *supra* note 5, at 1760 ("We can justify treating these entities differently using the language of duty and fault. Because large entropy reducers serve as one-stop shops for adversaries trying to link people to ruinous facts, they owe their data subjects a heightened duty of care.").

[305] Data Care Act of 2019, S. 2961, 116th Cong. § 3(a) (2019).

[306] *See* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 508 (2019).

[307] *See id.*

advertising survives these new digital fiduciary obligations, as has been suggested,[308] it is hard to imagine what exactly any new loyalty obligation would accomplish.[309] At any rate, no fiduciary duty currently exists to prevent tech companies from nudging vulnerable users to make unhealthy, profitable decisions. A digital information fiduciary regime seems impractical now, and prevention of health-detrimental nudges that encroach on user autonomy must come from other regulation.

[82] Finally, we should consider autonomy through the lens of bargaining power. Nudging has been criticized as a form of domination and exploitation of power dynamics.[310] But steering is just one form of coercion. Businesses also induce data sharing and collection through pay-for-privacy mechanisms like discounts and deals.[311] Companies like Google and Apple have spent years developing rich, proprietary ecosystems, making it more difficult for users to opt-out or switch products when they disagree with a company's data practices.[312] These power disparities are exacerbated by information asymmetries regarding data collection and use. Users are left in the dark regarding the how their medical data is being used, for what purpose, and how much data collectors stand to profit. Concerns over bargaining power will only increase if Big Tech firms turn into primary care providers or indispensable intermediaries in digital health economies. Regulation should account for how bargaining power affects user autonomy, recognizing that behavior modification tools are "susceptible to

[308] *See* Balkin, *supra* note 304, at 1220.

[309] *See* Khan & Pozen, *supra* note 306, at 511.

[310] *See* Will Legget, *The Politics of Behaviour Change: Nudge, Neoliberalism and the State*, 42 POL'Y & POL. 3, 10, 12–13 (2014) (describing the Foucauldian critique of nudging and behavioral modification).

[311] *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1387–92 (2017).

[312] *See* John M. Newman, *Antitrust in Digital Markets*, 72 VAND. L. REV. 1497, 1506–09 (2019).

abuse if they lack transparency, public visibility, and vigorous public scrutiny."[313]

3. Privacy and Sharing Protocols

[83] This Article has sketched much of the debate and competing considerations surrounding privacy in the new digital heath regime. This Section will summarize a few key takeaways. The new data-driven healthcare revolution implicates fundamental questions over patient and user privacy. Traditionally, the U.S. has treated medical privacy as exceptional and rigorously protected it. The digital healthcare regime threatens to upend the notion of medical privacy exceptionalism, as many new sources of medical information fall outside of the current regulatory landscape. Moreover, Big Tech's outsized role in developing digital health tools also gives cause for concern, given the tech companies' spotty record with user privacy. Despite this, a growing number of physicians have called for a reduction in patient privacy to facilitate a more efficient healthcare system. These physicians (and others) welcome new digital health tools, as they give unprecedented access to patients, and provide new opportunities to improve care. Finally, recent developments in data science have undermined HIPAA's reliance on deidentification. Healthcare privacy and healthcare research are now at odds with each other, and tradeoffs are inevitable. In this new health-privacy landscape, policy should not reflexively guard user privacy and limit data sharing. Rather, policy should be more contextual, and informed by other considerations like who benefits.[314]

[313] *See* BEAUCHAMP & CHILDRESS, *supra* note 295, at 235.

[314] *See* Price & Cohen, *supra* note 2, at 42 ("The future of big data privacy will be sensitive to data source, data custodian, and type of data, as well as the importance of data triangulation from multiple sources. But it is important that we not assume privacy maximalism across the board is the way to go. Privacy underprotection and overprotection each create cognizable harms to patients both today and tomorrow.").

4. Societal Analysis

[84] The final inquiry evaluates new digital healthcare tools at a societal level. The analysis is not directly related to "the interests of particular people" but rather to the "kind of society one wishes to live in."[315] Any policy should ask, regardless of the benefits, are there certain technologies or practices that should be disfavored or prohibited in a just society?[316] Whereas much of the analysis thus far has been utilitarian, the societal analysis serves as a dignitarian check during the evaluation of new digital health innovations, recognizing that "human dignity is a good which must not be compromised by our actions or practices and that any action or practice that compromises the good is unethical irrespective of welfare maximizing consequences."[317] This type of analysis should be more absolute and uncompromising compared to the previous levels evaluation. Technologies that fail this societal analysis will often be completely prohibited or banned. In the digital health paradigm, we are already seeing tools and practices that might be intolerable despite their potential benefits. For example, legislators around the globe are enacting and considering outright bans on certain types of facial recognition technology, given the

[315] Snelling & McMillan, *supra* note 292, at 86 ("[The] values invoked constitute more general ones that are not related to the interests of particular people, but rather involve appeals to intrinsic values and speak to the *kind* of society one wishes to live in. This is a much broader debate—one that is often triggered by new potentially 'transgressive' technologies that are thought by some to pose a threat to the moral fabric of society.").

[316] *See* ROGER BROWNSWORD & MORAG GOODWIN, LAW AND THE TECHNOLOGIES OF THE TWENTY-FIRST CENTURY: TEXT AND MATERIALS 8–9 (2012) (discussing how one should weight the benefits against the harms when deciding whether to patent particular sequences of human genomes).

[317] Roger Brownsword, *Bioethics Today, Bioethics Tomorrow: Stem Cell Research and the Dignitarian Alliance*, 17 NOTRE DAME J.L. ETHICS & PUB. POL'Y 15, 18 (2003).

possibilities for abuse, exploitation, and bias.[318]

[85] Societal analysis can also give regulators the chance to view new digital health care trends at a more abstract level. Rather than simply asking if the benefits of an individual device outweigh its harms, regulators could examine whether entire aspects of the digital health enterprise should be discouraged or prohibited. For example, policymakers may want to discourage self-tracking as a hobby, regardless of any benefit QSers receive, if it believes that self-monitoring should not be encouraged in a just society. More fundamentally, policy could ask whether a future healthcare system should be predicated on constant self-monitoring and corporate surveillance. Finally, regulators might contemplate whether Big Tech tools of prediction, personalization, and nudging are an impermissible encroachment on our free will and right to a future tense.[319]

B. Regulatory Requirements to Effectively Respond to the Digital Health Revolution

[86] For this analytical framework to be more than just abstract thinking, a number of conditions must be in place. Listed below are necessary prerequisites for any legislative response capable of adequately responding to new digital health technologies and practices. Namely, any new regulation must (1) have blanketed protection of data rather than a sectoral protection of health data; (2) allow for flexible and dynamic agency regulation of new and unanticipated digital health technologies and

[318] *See, e.g.*, Dave Gershgorn, *Maine passes the strongest facial recognition ban yet*, VERGE (June 30, 2021, 1:49 PM), https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law [https://perma.cc/K5VG-QNXR]; Foo Yun Chee, *EU privacy watchdogs call for ban on facial recognition in public spaces*, REUTERS (June 21, 2021, 9:09 AM), https://www.reuters.com/technology/eu-privacy-watchdogs-call-ban-facial-recognition-public-spaces-2021-06-21/ [https://perma.cc/L2M9-MPH9]; Kate Conger et al., *San Francisco Bans Facial Recognition Technology,* N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/49QW-P7UX].

[319] *See* ZUBOFF, *supra* note 66, at 331 (discussing how our right to the future tense is endangered by surveillance capital).

practices; and (3) have a focus and scope that extends beyond privacy protection.

1. Shifting from Sectoral Protection to Blanket Protection

[87] The digital health paradigm has decentralized collection and production of medical data. Inferences now allow for virtually any type of information to become health data. Together, these two developments have rendered obsolete the sectoral approach to health privacy. Yet, many new legislative proposals seek to simply expand HIPAA, rather than overhaul the way we regulate data. For example the proposed Protecting Personal Health Data Act attempts to remedy "key gaps that exist between HIPAA regulated entities and those not regulated by HIPAA," by covering "consumer devices, services, applications, and software . . . that are primarily designed for or marketed to consumers; and a substantial purpose or use of which is to collect or use personal health data."[320] However, the Act does not apply to "products on which personal health data is derived solely from other information that is not personal health data, such as Global Positioning System data. . . ."[321] Moreover, the only social media sites that are covered are those that "are primarily designed for, or marketed to, consumers to collect or use personal health data. . . ."[322] Exempt from regulation are Facebook Likes, Instagram filters, and all other non-medical data from which medical information can be inferred. The SMARTWATCH Data Act similarly enumerates types of consumer health information,[323] including personal biometric information,[324] and prohibits

[320] *See* Protecting Personal Health Data Act of 2019, S. 1842, 116th Cong. §§ 2(4), 3(1)(A)(i)–(ii) (2019).

[321] *Id.* § 3(1)(C)(i).

[322] *Id.* § 3(B)(iii).

[323] SMARTWATCH Data Act of 2019, S. 2885, 116th Cong. § 2(6) (2019) (defining consumer health information).

[324] *Id.* § 2(2)(A)–(B) (defining what is personal biometric information).

their transfer, sale, or sharing if individually identifiable.[325] These proposed acts fail to grasp how radically the health information paradigm has been transformed by Big Data and Big Tech. Updating HIPAA and relying on similar types of safeguards will undoubtedly leave sensitive health data exposed, like medical inferences, risking obsolescence before enactment. Any sectoral regime will eventually devolve into a whack-a-mole strategy, leaving gaps in legislation.[326]

[88] Instead, a more comprehensive data approach is necessary to fully respond to the digital health revolution. Many have suggested that federal U.S. privacy law incorporate blanket data protections akin to the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).[327] The GDPR covers anyone that processes personal data, including individuals and nonprofit organizations.[328] Focusing on the act of processing data, rather than the type of data, leads to less balkanized data protection, reducing the chance that medical data will fall through the cracks and go unprotected. The CCPA, while still less sectoral than the current U.S. federal privacy regime, is not as all-encompassing as the European system. It "applies only to businesses, and only to those that meet

[325] *Id.* § 3(a)(1).

[326] *See* Ohm, *supra* note 5, at 1742.

[327] *See, e.g.*, *Facebook is Not the Problem. Lax Privacy Rules Are.*, N.Y. TIMES (Apr. 1, 2018), https://www.nytimes.com/2018/04/01/opinion/facebook-lax-privacy-rules.html [https://perma.cc/GN2N-PFFN] (calling for a GDPR-approach to privacy); Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/F634-2FZ8]; Daniel J. Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACHPRIVACY (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/ [https://perma.cc/WV8A-WHRN].

[328] Directive 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 26 (EU); Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1758 (2021).

a complex set of overlapping requirements related to their size or the extent of their involvement in personal data trade."[329] Both the CCPA and GDPR have tiered schemes that impose heightened standards for larger data collectors.[330] A few data legislative proposals have incorporated the blanket approach. The Data Care Act, though only applying to online service providers, focuses on sensitive data of many types, and is not limited to a given context.[331] The Mind Your Own Business Act would apply to any "person, partnership or corporation" under the jurisdiction of the FTC that meets a number of size-based criteria.[332]

[89] Blanket data protections are essential in any framework to address the digital healthcare revolution. Without control over all types of data, regulation will continue to be patchy and inadequate to respond to emerging sources of medical information. Of course, blanket protections are not answers on their own; simply having the power to regulate these data sources does not solve how to balance interests at the core of health privacy law. Moreover, current blanket data legislation is not perfect. For instance, under the GDPR, inferences are considered the "economy class" of personal data.[333] While data input protections are strong, the "few mechanisms in

[329] *See* Chander et al., *supra* note 328, at 1758.

[330] *See* Council Regulation 2016/679, *supra* note 328, at 3 ("To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping.").

[331] *See* Data Care Act of 2019 § 2(4)–(5) (2019).

[332] Mind Your Own Business Act of 2019, S. 2637, 116th Cong. § 2(5)(A) (2019) (stating covered entities must have "greater than $50,000,000 in average annual gross receipts for the 3-taxable-year period preceding the most recent fiscal year . . . or posses[] or control[] personal] information on more than – 1,000,000 consumers; or 1,000,000 consumer devices").

[333] *See* Wachter & Middelstadt, *supra* note 239, at 499 (stating "[d]ata subjects' rights to know about (Art. 13–15), rectify (Art. 16), delete (Art. 17), object to (Art. 21), or port (Art. 20) personal data are significantly curtailed when it comes to inferences, often requiring a greater balance with the controller's interests (e.g., trade secrets or intellectual property)" than would otherwise be the case.).

European data protection law that address the outputs of processing, including inferred and derived data, profiles, and decisions, are far weaker."[334] Considering the importance of inferences and prediction in digital healthcare, weak protection for inferences could undo any health data legislation. Ultimately, blanket data protection should be viewed as necessary, but not sufficient to respond to the digital health paradigm.

2. Flexible and Dynamic Regulation over New Practices

[90] In only a few years, technology companies have flipped traditional medical systems on their head, ushering in a new era of digital health. Still, the industry is only in its infancy. Practices and technologies are rapidly being developed. Tools that seem essential to data-driven healthcare systems could become obsolete in a few years. Given the unpredictability and instability of this nascent health paradigm, regulators must have the authority and ability to quickly respond to sudden changes. Congress cannot repeat the mistakes of HIPAA, when it left the crucial regulatory indicators like PHI largely unchanged for decades.[335] Rather, agencies, whether the FTC or HHS, must have the power to quickly evaluate and respond to new tech practices.

3. Thinking Beyond Privacy Protection

[91] Thus far, most of the discussion surrounding data-driven medical tools primarily focuses on privacy concerns.[336] New legislative proposals to update and extend HIPAA assume that the digital healthcare revolution only

[334] *Id.* at 514.

[335] *See* Ohm, *supra* note 5, at 1731–32.

[336] *See, e.g.*, Price & Cohen, *supra* note 2, at 37 ("We begin by discussing the benefits big data may bring to health science and practice, before turning to the concerns big data raises in these contexts. We focus on a prominent (but not the only) worry: privacy violations."); Mehmet Kayaalp, *Patient Privacy in the Era of Big Data*, 35 BALKAN MED. J. 8, 8 (2018); Frank A. Pasquale & Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 595–96 (2014).

affects user privacy.[337] However, this article has demonstrated that new health technologies and practices raise fundamental questions of autonomy, bargaining power, fairness, and dignity. Any proposed solution that does not adequately account for these dimensions will leave many of the most significant dangers posed by the new paradigm unaddressed.

[92] Policymakers should take tips from the GDPR and CCPA for ways to respond to non-privacy values in privacy-focused legislation. For example, both the GDPR and CCPA require varying degrees of user consent for data collection. The GDPR requires affirmative opt-in on behalf of users for any data processing to be lawful,[338] whereas the CCPA allows users to opt-out of data collection.[339] These mechanisms are an explicit thumb on the scale for user autonomy and bargaining power. In another instance, Proposition 24, a California state initiative that updated the CCPA, expanded "pay-for-privacy" mechanisms that were absent in the original CCPA. The new pay-for-privacy scheme has been called inequitable, placing an undue burden on lower-income consumers who are forced between protecting their information or essentially paying a privacy tax.[340]

---

[337] *See* Protecting Personal Health Data Act of 2019 § 3(1)(A)–(C); Mind Your Own Business Act § 2(1)–(4); SMARTWATCH Data Act of 2019 § 2(5)–(6).

[338] *See* Council Regulation 2016/679, *supra* note 328, at 7–8 ("In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.").

[339] *See* CAL. CIV. CODE §1798.120(a) (West 2020) ("A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.").

[340] *See* Greg Besinger, *A Privacy Measure That's Hard to Like*, N.Y. TIMES (Oct. 28, 2020), https://www.nytimes.com/2020/10/28/opinion/california-prop-24-privacy.html [https://perma.cc/ZX6W-4F3D]; *Prop 24: Consumer Data Privacy*, LEAGUE WOMEN VOTERS CAL., https://lwvc.org/vote/elections/ballot-recommendations/prop-24consumer-data-privacy [https://perma.cc/25B5-6S6K] ("Among the troubling aspects of Prop 24 is its expansion of 'pay for privacy' through the addition of loyalty and rewards programs, allowing businesses to charge consumers more or provide worse service if they choose to exercise their privacy rights. The initiative also allows businesses to require consumers to

Pay for privacy, while clearly implicating privacy issues, also touches on fairness and equity. Federal data legislation must account for similar considerations, even if regulation primarily addresses health information and privacy concerns.

VI. CONCLUSION

[93] Big Data and Big Tech have irreversibly changed the way we view and approach healthcare. Now, companies and medical providers have constant access to users and patients, thanks to a wave of consumer healthcare devices. Hospitals and traditional healthcare providers can apply data-driven techniques to medical care, treatment, and research. New progress in data analytics has the potential to turn virtually every social media post into medical information.

[94] With this transformation comes uncertainty and the potential for harms. These new practices implicate issues of privacy, bias, inequity, and autonomy. We have already seen abuse and vulnerabilities in this decentralized and currently unregulated healthcare system. Yet, legislators should not reflexively deem digital health innovations a threat. Real, tangible benefits from a data-driven medical system exist. Policymakers must address regulation of new devices in a holistic manner, evaluating all of the potential harms and benefits of these health tools. From this lens, legislation can best guide a 21st-century approach to both healthcare and data protection.

direct each individual website and app not to sell information - weakening the current legal requirement that companies respect a global opt-out for all services. These burdens are fundamentally inequitable, placing the onus on the average consumer to protect their own privacy.").