Dear colleagues: I sincerely appreciate your thoughts on this very early-stage work. This is the first of two papers that will be written to be somewhat referring. The first is "Prescribing Exploitation," while the second is "Prescribing Discrimination." The second paper develops further the concepts of autonomy, dignity, datafication, and expediency with a coauthor who studies human-computer collaboration, Dr. Krista Kennedy. This is intended to address some of the existing legal issues and scholarship without digging too deeply into the philosophical side of the question. Please forgive my shoddy footnotes in this early draft! I welcome your thoughts!

Best Regards,

Charlotte Tschider

Loyola University Chicago School of Law

Prescribing Exploitation

"Since mankind's dawn, a handful of oppressors have accepted the responsibility over our lives . . . By doing so, they took our power. By doing nothing, we gave it away."[1]

Charlotte A. Tschider

Abstract

Patients are increasingly reliant temporarily, if not indefinitely, on connected medical devices and wearables, many of which use artificial intelligence (AI) infrastructures and physical housing that directly interacts with the human body. The automated systems that drive the infrastructures of medical devices and wearables, especially those using complex AI, often use dynamically inscrutable algorithms that may render discriminatory effects that alter paths of treatment and other aspects of patient welfare. As a result, many scholars across disciplines have explored the nature of such discrimination, while legal scholars have sought to recommend preventative or responsive actions to address these socially damaging results.

These contributions, though important, reinforce existing models of discrimination, precisely statutorily established discrimination categories. This research, however, has not examined how AI technologies animate exploitation of medical technology users and, in some cases, create new types of discrimination through their use. Health data discrimination results from a combination of factors essential to effective medical device AI operation: 1) existence of a fiduciary relationship or approximation, 2) a technology-user relationship that does not involve the expertise of the fiduciary, 3) existence of a critical health event or health status requiring use of a medical device, 4) ubiquitous sensitive data collection essential to AI functionality, 5) lack of reasonably similar analog technology alternatives, and 6) compulsory reliance on a medical device.

This paper makes two key contributions to existing literature. First, this paper establishes the existence of a type of exploitation and, under some circumstances, discrimination, which is not simply exacerbated by technology, but new forms of differential treatment and exposure created by its use. Second, this paper applies Frank Pasquale's updated description of the information fiduciary, explaining how such a model could work to avoid discrimination.

[1] ALAN MOORE, V FOR VENDETTA (DC Comics: 1989).

CONTENTS

INTRODUCTION

Patients are increasingly reliant temporarily, if not indefinitely, on connected medical devices and wearables, many of which use artificial intelligence infrastructures and physical housing that directly interacts with the human body. Many individuals who have used or been treated by compulsory medical devices have been members of legally protected groups specifically enumerated in anti-discrimination law, such as disability status.

The automated systems that drive the infrastructures of connected medical devices, especially complex AI, often use dynamically inscrutable algorithms that exploit patients and may render discriminatory effects that alter paths of treatment and other aspects of patient welfare.[2] As a result, many scholars across disciplines have explored the nature of such discrimination, while legal scholars have sought to recommend preventative or responsive actions to address these socially damaging results.

These contributions, though incredibly important, reinforce notions of discrimination focused on predefined groups, and AI discrimination and unfairness work scrutinizes immediate and harmful decisional effects on predefined communities and groups, such as race, ethnicity, religion, gender, sexual identity, or disability status and proxies for these statuses.[3] This research, however, has not examined how artificial intelligence can create new and exacerbating types of discrimination through exploitation: discrimination based on substantial and pervasive loss of privacy, *technological discrimination*. Technological discrimination is the cumulative effect of power differentials, trust deficiencies, and opacity, concerns that have occupied privacy and fairness literature for some time.

In healthcare, exploitation results from a combination of factors essential to effective medical device AI operation that nevertheless make an individual reliant almost exclusively on a health care organization:[4]

---

[2] Jenna Wiens et al., *Diagnosing Bias in Data-Driven Algorithms for Healthcare*, 26 NATURE MED. 25, 25-26 (2020).

[3] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 675 (2016); Anya E.R. Prince & Daniel Schwarcz [hereinafter, Prince & Schwarcz], *Proxy Discrimination in the Age of Artificial Intelligence*, 105 IOWA L. REV. 1257, ? (2020).

[4] It should be noted that although this Article focuses on the healthcare sector, the exploitation of the individual that brings about technological discrimination is not unique to healthcare. Indeed, exploitation may present itself differently in different commercial sectors and between different types of actors, as between the government and those accused or convicted of crimes. This Article aims to illustrate how the technological discrimination result functions to create a disproportionate burden on a portion of the population, and further burdening those already burdened by the invisible structures that perpetuate discrimination.

1) Existence of a critical health event or health status requiring use of a medical device;
2) Compulsory use of a medical device;
3) Ubiquitous sensitive data collection essential to AI functionality and corresponding AI opacity;
4) Existence of a fiduciary relationship or approximation of a fiduciary relationship that gives an appearance of expertise and trust;
5) A technology-user relationship that does not involve the expertise of the fiduciary, as is frequently the case in AI technologies doctors do not fully understand;
6) Lack of reasonably similar analog technology alternatives, limiting options in controlling data about oneself

Each of these factors increase the probability of *technological discrimination*, or a deontological privacy risk resulting from healthcare AI use.[5] When patients reliant on medical device AI are disproportionate and unreasonably exposed to substantially more privacy risk than their peers, they may be subject to a new form of discrimination. If individuals who are compulsorily dependent on AI-enabled healthcare technologies are uniquely vulnerable relative to their non-technology-dependent peers, they may be owed additional duties to reduce such risks to an acceptable level.

Consider the following example:

> *Gildas is deaf and has been a hearing aid wearer for most of their life, since experiencing a labyrinthine concussion from an explosion while growing up during the Second Congo war. When Gildas moved with their family to the United States, Gildas received their first hearing aid, but the first hearing aid amplified all of the environmental sounds, causing serious ringing and pain for Gildas. Gildas has used a masking device instead of a hearing aid most of their life, but Gildas' hearing never returned, causing serious issues in Gildas' education and opportunities. Gildas recently started college, and after meeting with their physician, Gildas became aware of a new AI-enabled hearing aid that could operate both as a mask and in amplifying certain sounds to help Gildas hear their professors' lectures more easily.*[6]

At first glance, this is a feel-good story: a patient will receive a medical device that will transform their learning experience. However, upon

---

[5] I. Glenn Cohen & W. Nicholson Price II, *Privacy in the Age of Medical Big Data,* 25 NATURE MED., no. 1, 2019 at 37–43.

[6] This scenario is based on a recent study that involved mapping information ecologies for hearing devices. *See* Krista Kennedy, Charlotte A. Tschider & Noah Wilson, *Balancing the Halo: Algorithmic Secrecy and Data Surveillance Disclosure in Medical Devices*, 4 RHETORIC OF HEALTH AND MED., no. 1, University of Florida Press (2021).

closer look, the patient is likely exposed to substantial privacy risk. The doctor or an audiologist likely does not know how data from the patient are used and cannot explain these practices to the patient, such as collection and retention of environmental and location data, identities of the patients' contacts, and even the patient's music playlist, helpfully integrated with the hearing aid app on their mobile device. These data are transferred as identifiable personal information along with a wide variety of other lifestyle data to back-end manufacturer systems.

Although the features of such a product may be knowable, the ways in which the product makes decisions about the wearer are not. These systems may use AI algorithms that often learn in an unsupervised, unlocked, continuous learning environment, an environment the manufacturer likely outsources to a third party whose algorithms the manufacturer cannot explain or understand. These data may be transferred to additional third parties, such as a cellular provider, mobile device manufacturer, or data collated between users and sold to data brokers. What meaningful choice does Gildas have? Should Gildas have to choose between a medical decision that, from Gildas' perspective will improve their quality of life, and their privacy?

As a result of data collection for an arguably necessary and continuously wearable medical device, Gildas will be rendered a digital approximation of themselves, datafied, disembodied and potentially subject to data overuse.[7] Gildas may also be subject to greater *consequentialist* risk, such as increased risk of impersonation and fraud, and unauthorized access or disclosure of sensitive data.[8] If Gildas is already subject to a greater risk of discrimination based on Gildas' immigrant status, race, disability status, religion, or identity, such as via black-box algorithms that may be trained on discriminatory data sets or render an unfair results, technological discrimination will multiply or exacerbate existing discriminatory effects, a type of multiplier.

This paper makes two novel contributions to AI ethics and privacy literature. First, this paper proposes the recognition of a new form of discrimination not exacerbated by privacy issues but *created* by them, wherein an individual's significant exposure to continuous surveillance and exploitation results in compromised privacy interests. Second, this paper applies a model for preventing technological discrimination where technological discrimination is likely to occur, such as the healthcare sector, and explores how such a model could be implemented. This model builds Frank Pasquale's adaptation of Jack Balkin's proposed

[7] *See* infra, Part III, describing datafication and natural tendency to remove the "personal" from personal information in large data sets.
[8] *See* supra notes 5, 6, and 7.

information fiduciary concepts,[9] which have been circulated widely through the information privacy community, to a subset of automated technologies in the health sector and the data they process.

This paper proceeds in four parts. Part I describes the contemporary nature of health technology and health data use that creates the scaffolding for technological discrimination, including big data, advanced diagnostics, mobile health technologies, medical devices, and Internet of Health Things (IoHT). Part II examines key issues with healthcare technologies and the healthcare sector overall, exploring the factors that increase the likelihood of exploitation and, in some cases, technology discrimination. Part III explores the foundations of trust and misplaced trust within the healthcare technology ecosystem, then describes the broad call for information fiduciaries within relationships of trust. Part IV illustrates how an information fiduciary approach to preventing discriminatory impact may prevent the exacerbation of existing and mobilization of new forms of discrimination. I further propose a framework for determining when an information fiduciary role may be appropriate in the healthcare sector.

PART I: CONTEMPORARY HEALTHCARE TECHNOLOGIES

AI is often depicted as the future, but AI is being used today. From self-driving cars to advanced medical robotics, AI is being used—often surreptitiously—by a wide variety of organizations and product manufacturers. AI may take various forms, whether automating processes, improving human decision-making, improving safety and efficacy, democratizing expertise, or driving optimal machine functionality. AI may be embodied in robotics, connected to sensors and other kinetics, or it may be disembodied, as in software and mobile apps.

Healthcare, a sector that stands to benefit from increased efficiency, quality, and cost, is positioned to embrace AI and connected technologies as a means of providing more, better, and cheaper healthcare, a triad of goals usually not satisfied without sacrificing the others. Health technology, in the form of big data, artificial intelligence, consumer wearables, and medical devices, *could* revolutionize the practice of medicine—if the U.S. can do so without additional risk to the very people who stand to benefit.

[9] Frank A. Pasquale, *Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society*, 78 OHIO STATE L. REV. 1243 (2017).

A. Big Data – Healthcare Providers, Insurers, Employers

The terminology "big data" is used heavily in a variety of sectors to describe exceptionally large data sets. Big data may be used for purposes including advanced analytics, organizational operations optimization, and innovation. And yet, data are just data: information encoded in 0s and 1s in their most primitive form.

Despite their objectively inauspicious form, data are powerful. Because data encode information about our world, about our bodies, they are tremendously valuable, in aggregate and in relation to the individual to facilitate technology personalization. Data matter because of what they can tell us about ourselves, about our organizations, and about the world around us. Functionally speaking, data do not usually matter because of *what they encode*, but rather *what they can tell us* about the underlying systems that motivate our lives.[10] Information exists simply by being, by living in a world, by making decisions. But *data* exist because we *choose* to document it.

Big data and its applications into mobile technologies, advanced analytics, and artificial intelligence, have changed our lives because more and more information about our lives is being recorded—and, presumably, has value—to someone.[11] Artificial intelligence and advanced analytics seek to tell us something about the world around us or our inner biological functions, in a much more comprehensive fashion than ever before, maximizing use of the machines that have always captured and recorded data, but in a way that does not superimpose human perceptions of how underlying systems work. Consider the following example:

> *Gelena has struggled with gastrointestinal issues all of her life. As a young child, Gelena's father gave her glasses of milk to settle her stomach, which sometimes caused vomiting. After removing dairy from her diet, Gelena's symptoms improved. At age 10, Gelena began experiencing rectal bleeding, which a doctor determined was from a form of colitis. After completing a combined upper GI endoscopy/colonoscopy, however, the doctor identified some intestinal inflammation but not the type of inflammation usually associated with colitis. At age 14, Gelena began having problems eating wheat products and was diagnosed by another doctor with celiac disease. After removing wheat from her diet, Gelena managed not to have any serious medical issues until recently. Now 22 years old, Gelena has begun having nausea and serious stomach*

[10] W. Nicholson Price II & Arti K. Rai, *Clearing Opacity through Machine Learning*, 106 IOWA L. REV. 775 (2021).
[11] ADAM TANNER, OUR BODIES, OUR DATA (Beacon: 2017).

pain. Another doctor completed a full endoscopy/colonoscopy again and some blood tests, she determined that Gelena has gastroparesis. Although Gelena is managing her gastroparesis by avoiding certain foods and taking some pharmaceuticals to reduce the symptoms, there is no cure. At this time, Gelena is not able to maintain employment or care for her child due to the seriousness of her symptoms.

The example above illustrates the type of situation where big data using AI diagnostic algorithms could be useful. In each one of the physician interactions, the physicians could only diagnose the condition based on the information and tools available to them at the time, usually information provided by the patient. If data could be collected on an ongoing basis, real-time, directly from Galena's body and using data Galena inputs into an app (what she ate and when, timing of digestive processes, and symptoms), perhaps doctors could better determine the cause of her health issues.[12]

However, more data does not necessarily mean better results. There is the real challenge of organizing data in such a way that it can be useful. If data are collected from Galena's body via blood draws, Gastro-intestinal (GI) imaging, Barium X-rays, self-reported information, and a device like the PillCam™[13] and organized effectively, the probability of determining the root cause of Galena's illness increases, whether or not advanced AI technology is used. Although GI experts might be able to immediately determine Galena's problem from a multitude of data points, not all physicians have this expertise and not all patients like Galena have access to experts.[14] The solution may be creating health AI that can mine and analyze a significant volume of data, from various health care providers and technologies.[15]

Imagine how much data might be collected through various tests, systems, and input by Galena in a mobile app. The probability of successfully mining the data to render an accurate diagnosis would likely increase substantially if computational resources can evaluate relationships within a large volume of structured data. Based on data collected from patients like Galena, latent relationships between not only two data points but hundreds of thousands could improve diagnostic

---

[12] Indeed, any one of these inputs could be useful for diagnostics, which is why mobile device apps and patient self-monitoring has become an important intermediary step for more effective diagnostics.

[13] PillCam™ SB 3 System | Medtronic

[14] W. Nicholson Price II, *Medical AI and Contextual Bias*, 33 HARV. J. L. & TECH. 66 (2019), Medical AI and Contextual Bias | Petrie-Flom Center (harvard.edu).

[15] Charlotte A. Tschider, Legal Opacity: Artificial Intelligence's Sticky Wicket (Iowa Law Review 2021, forthcoming). Limitations on data use and transfer subject to contracts may impede data collation for purposes like this. *See also*, supra note 14, at X (describing the risk of exporting expertise without considering the health context of such application).

effectiveness. This is the type of function AI utilities can provide, with the potential to render (with sufficient data) a probabilistic determination such as "98% likelihood of Crohn's Disease" in less than a minute for an area of medicine that is notoriously difficult to accurately diagnose.[16]

Data and the infrastructure used to organize, mine, and analyze data are symbiotic: AI is rendered useless without adequately representative data. And data without infrastructure are not useful, either.[17] And data are less useful without the machinery to mine and analyze them. Similar to clinical trials, insufficient data renders statistical analysis ineffective, unfair, even dangerous. Combined big data sets, with different organizational provenances, are both highly desirable commercially and necessary for effective health technology to operate, whether mobile technologies, Internet of Health Things, or AI-enabled technologies.[18]

Medical devices using such data usually consist of five technological components: sensors, sensor fusion and algorithmic inferences, connectivity, infrastructure, and (for some medical devices) mobility and miniaturization.[19] It is the transition between the physical and the digital world that makes these devices potentially problematic from a privacy and security perspective, leading to the potential for physical injury, exploitation, or manipulation of individuals dependent on these devices.[20]

Indeed, many of these devices are not owned by the patient or even the organization operating them, and data produced by the human-device collaboration are not owned by the patient interfacing with the device.[21] Medical device manufacturers are rarely non-profits, and to some degree, patients are exploited for their data, exploitation that is often framed as part of a legitimate exchange: to benefit from the technology, you must

---

[16] Artificial intelligence in gastrointestinal endoscopy: general overview (nih.gov)

[17] Nicholson Price Contextual Data piece; note 10 above; Selbst and Barocas; Prince and Schwartz; Tschider BYU piece.

[18] "Provenance" is used to determine from whom and where data originated. Data provenance is a concern for nearly all data implementations, as once data are collected often they are transferred to other parties without information about their origin attached. This causes significant issues for contract compliance and privacy laws that may prohibit data use under some circumstances.

[19] JOSHUA A.T. FAIRFIELD OWNED PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM 54-62 (Cambridge Univ. Press: 2018).

[20] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014), *available at* https://scholar.law.colorado.edu/articles/83; Charlotte A. Tschider, *Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. L. REV. 87 (2018); Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace, 26 Annals Health L.* 1 (2017); Charlotte A. Tschider, *Deus ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future*, 5 SAVANNAH L. REV. 177 (2018); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Tschider, supra note 31.

[21] *See* supra note 19, at 2-3 (describing the simultaneous intrusion of devices into the most personal environments coupled with control over assets and data, a 'digital serfdom'); Krista Kennedy, *Designing for human-machine collaboration: Smart hearing aids as wearable technologies*, 5 COMM. DESIGN QTRLY., 40, 40 (2017).

provide your data.[22] If a patient desires to manifest some choice over the situation, all a patient really has are privacy interests which, as we will see, are riddled with foundational problems.

B. Artificial Intelligence in Medical Technology

Artificial intelligence is used in any variety of medical applications. From more effective quality evaluation to enable Accountable Care Organizations to operational efficiencies, AI is being used to decrease costs while improving care. However, the most promising AI applications are those poised to save lives and dramatically improve the quality of patients' lives. Four areas where AI may be especially useful are in medical wearables, implantable devices, medical diagnostics, and AI robotics.

1. Medical Diagnostics: Arterial Imaging

One area of increased focus for AI is medical diagnostics. Although a variety of different medical diagnostics are seeing significant development and investment, medical imaging AI has received much attention in its ability to augment and improve the effectiveness and efficiency of radiological interpretation.[23] Arterys is one example of successful companies in AI radiological interpretation, though AI products are combining common medical procedures with diagnostics, such as lesion detection in colonoscopies.[24]

Arterys has created an AI platform that integrates with existing arterial imaging technologies, such as MRIs, CT scans, and X-rays.[25] To date, Arterys has developed platforms that focus on four major medical diagnostic areas: Cardio, Lung, Chest, and Neuro.[26] Importantly, Arterys claims to have implemented such a system and promoted data sharing while protecting individual privacy,[27] a uniquely difficult feat in imaging generally.[28]

Arterys' approach has been to amplify physician effectiveness through "human + AI."[29] Arterys created 4D flow technology in an accessible, Web-based format so that physicians can better visualize bloodflow in

---

[22] *See* supra note 19, at 89-90.
[23] Frontiers | Artificial Intelligence for the Future Radiology Diagnostic Service | Molecular Biosciences (frontiersin.org)
[24] FDA Authorizes Marketing of First Device that Uses Artificial Intelligence to Help Detect Potential Signs of Colon Cancer | FDA
[25] Medical Imaging Cloud AI - Arterys
[26] *Id.*
[27] *Id.*
[28] Medical Imaging and Privacy in the Era of Artificial Intelligence: Myth, Fallacy, and the Future - PubMed (nih.gov)
[29] *See* supra note 25.

arteries. Arterys' products consistently identify portions of the images that illustrate issues rather than relying on more subjective, static image diagnostics.[30] In 2017, this technology received the first-ever U.S. Food & Drug Administration clearance for cloud computing and AI deep learning in a clinical setting.[31] Arterys has also extended and enhanced its uses by encouraging AI developers to upload algorithms for specific applications.[32]

2. AI Surgical Robotics: The CyberKnife

Surgical robotics has transformed surgery as we know it, primarily developing minimally invasive surgical techniques for surgeries that require a greater degree of precision and control.[33] Minimally invasive surgeries using surgical robotics usually claim fewer complications, including site infection, faster recovery, less pain, less blood loss, and smaller scars.[34] Surgical robots do not operate independently—they are designed to be used by a surgeon who has been trained to use the surgical robot. Surgical robots, however, use AI to determine surgical patterns and calculate appropriate angles and distances because surgical robotics often work on a smaller plane than traditional surgeries, working in distances that cannot be gauged with the naked eye, in submillimeters.[35]

The Computer Motion AESOP machine became the first FDA-approved robotic surgical medical device for endoscopic medical procedures in 1990.[36] But the most significant evolution in robotic surgery began in 2000 with the da Vinci surgical system, which was approved for general laparoscopic surgery, and can be used for both adult and pediatric surgery.[37] The da Vinci introduced centimeter-thick arms and a three-dimensional visualization screen, enabling less contact with interior tissue, reducing the risk of infection. The "Endo-wrist" function precisely replicates the movement of surgeons themselves.[38] This physical housing

---

[30] About Us - Arterys

[31] *Id.* It should be noted that Arterys went through a 510(k) clearance process, which is a truncated review for low-risk AI, which may or may not accurately evaluate potential issues. Charlotte A. Tschider, *Medical Device Artificial Intelligence: The New Tort Frontier*, 46 BYU L. REV. 1551 (2021), Medical Device Artificial Intelligence: The New Tort Frontier by Charlotte Tschider :: SSRN (describing broad issues in tort recovery when devices have been reviewed by the FDA and the insufficiency of such a review).

[32] Marketplace - Arterys. At the time of writing, Arterys had four commercialized algorithms, with 44 non-Arterys algorithms on their Website, some of which have been "FDA cleared," CE Mark (the EU FDA model for medical devices), or KFDA approved (the Korean FDA), while others are for research purposes only.

[33] Robotic surgery - Mayo Clinic

[34] *Id.*

[35] Robotic Surgery: The Role of AI and Collaborative Robots (automate.org)

[36] History of Robotic Surgery and FDA Approval - Robotic Oncology

[37] *Id.*

[38] *Id.*

has inspired the coupling of advanced kinetic movement and haptic sensors with artificial intelligence to perform more effective surgical techniques and, in limited use cases, autonomous surgery.[39] The inclusion of AI in surgical robotics is highly variable, from some assistance to full automation.[40]

Artificial intelligence in surgical robotics enables two key functions: the preprogrammed goal and its ability to dynamically respond to the ever-changing surgical environment.[41] Preoperative planning is used prior to surgery commencing and consists of medical imaging AI and medical record data to determine how the surgical robot will be used.[42] Spatial landmarks and alignment between medical imaging sources determine the surgical field and feed into the surgical robot's preprogramming before surgery.[43] During surgery, AI converts the surgical field interior to a patient's body into a 3D rendering for physician visualization, differentiating tissue types, and estimating and executing surgical navigation.[44]

One example of AI-enabled surgery that combines advanced imaging and robotic treatment is the ACCURAY CyberKnife® S7™ System (CyberKnife).[45] The CyberKnife delivers stereotactic radiosurgery (SRS) and radiation therapy to treat various forms of cancer.[46] The CyberKnife is different from typical robotic surgery in that the CyberKnife can deliver non-surgical stereotactic treatments in sub-millimeter accuracy on numerous organs: prostate, liver, brain, lung, spine, kidney, or pancreas.[47] The CyberKnife receives real-time imaging during radiation treatment, approaching tumors from thousands of angles to deliver radiotherapy to precisely the tissue that needs it. CyberKnife AI reduces the effects on healthy tissue and improves post-surgical recovery and reduces overall side effects.

3. Implantable Devices: Insulin Pumps

Implantable devices, sometimes called implantable electronic medical devices (IEMD) increasingly use AI both to train devices for more effective use and to routinely update their safety and efficacy based on new data supplied to the algorithms that inform device function and

---

[39] Artificial Intelligence and the Future of Surgical Robotics : Annals of Surgery (lww.com).
[40] *Id.*
[41] *Id.*
[42] Application of artificial intelligence in surgery - PubMed (nih.gov), at 418-19.
[43] *Id.*, at 419.
[44] *Id.*, at 419-20.
[45] Homepage | Accuray Radiotherapy
[46] *Id.*
[47] *Id.*; CyberKnife SRS / SBRT System from Accuray

precision.[48] There are a wide variety of implantable devices currently on the market, such as brain stimulation devices, pacemakers, gastric stimulators, and insulin pumps. Prosthetic limbs controlled through a brain-machine interface (BMI) have also received significant recent attention.[49]

One implantable or permanently affixed device beginning to use AI is the insulin pump, commonly used for Type 1 diabetes management. Insulin pumps eliminate the need for direct insulin delivery using insulin syringes and are increasingly used for children, who benefit from continuous glucose monitoring and automated delivery. Despite the invention of the insulin pump, individuals with Type 1 diabetes still struggle to achieve their glycemic goals, which has opened the door to AI-enabled insulin pump systems.[50]

The FDA granted DreaMed's Advisor Pro (Advisor Pro)'s de novo request in 2018.[51] The Advisor Pro is an AI-enabled decision-support tool. DreaMed's decisional support tool is fueled both by endocrinologist expertise and real-world use.[52] Data are collected both from the insulin pump itself and other devices, such as the self-monitoring of blood glucose (SMBG) and continuous glucose monitoring (CGM).[53] These data are then analyzed by the MD Logic algorithm, which suggests optimization of basal rate, carbohydrate ratio (for diet), insulin sensitivity, and personalized diabetes management tips.[54]

4. Medical Wearables: Smart Hearing Aids

Smart hearing aids have hit the market, poised to revolutionize the social and economic lives of millions of Americans. Hearing aids are used by individuals of all ages in a variety of communities with different lifestyle needs. The hearing needs of an individual who is retired, active, and social are drastically different from a child in a school classroom and on the playground or a professor attending academic conferences. Often doctors refer a patient to an audiologist who can help to personalize settings and educate patients about the features of their aid.[55]

---

[48] Part human, part robot: The future of medical implantables | Pursuit by The University of Melbourne (unimelb.edu.au)
[49] *Id.*
[50] Insulin dose optimization using an automated artificial intelligence-based decision support system in youths with type 1 diabetes - PubMed (nih.gov)
[51] How AI Is Personalizing Insulin Therapy for Diabetes Patients (mddionline.com)
[52] AdvisorPro_Brochure.pdf (dreamed-diabetes.com)
[53] *Id.*
[54] *Id.*
[55] Kennedy Tschider Wilson article balancing the halo. On SSRN and here behind a paywall Balancing the Halo | Rhetoric of Health & Medicine (ufl.edu)

The Starkey livioEdge^{AI} (Livio) is one example of such aids.[56] The Livio claims best in class listening through its AI-based learning system that adjusts to your surroundings to provide the best listening experience possible, "Edge Mode."[57] The Livio also provides monitoring support for older adults. With the Livio, Starkey introduced integrated sensors, which can detect when an individual falls and may have seriously hurt themselves. The alert system then sends an automatic message to designated people to notify them of the fall.

The Livio is compatible with mobile devices, which integrates features of the device through the Thrive Hearing Control mobile app that also includes brain and body activity tracking, the Intelligent Assistant, and Mask Mode to enhance hearing when individuals are wearing masks.[58] The Intelligent Assistant provides voice recognition and Smart assistance, similar to Alexa or Siri.[59] The Livio's "easy personalized control" boasts the device's ability to adjust to an individual's unique lifestyle.[60] Ultimately, the Livio is designed to be worn continuously while seamlessly interfacing with not just the wearer's physical body but also their lifestyle.

These AI technologies demonstrate the potential for substantial medical improvements through technology advancement. AI technology has the potential to improve the effectiveness of medical treatment, from diagnosis to treatment for a point in time, to pervasive medical condition management. These technologies demonstrate not only the wide variety of medical products now available but also the importance of data both in creating the algorithms that run these technologies and in optimizing their function over time.

PART II: THE "NATURE" OF HEALTHCARE TECHNOLOGY DATA

Despite their relative point-in-time or continuous use, all medical device types described in Part I require data, including highly sensitive personal information, to 1) create the algorithms used, 2) to provide real-time adjustments for more effective device use, and 3) to provide personalized delivery of healthcare.[61] Machine learning algorithms cannot be created without data and depend on continuous feeding to improve their effectiveness.[62] Data *essentialism* motivates ubiquitous data collection:

---

[56] AI Powered Hearing Aids | Starkey Livio Edge AI
[57] *Id.*
[58] Thrive Hearing Control App | Starkey; STARKEY (hereinafter, Starkey AI), AI Powered Hearing Aids | Starkey Livio Edge AI.
[59] *See* Starkey AI, supra note 58.
[60] Thrive Hearing Control App | Starkey
[61] Tschider, *Legal Opacity: Artificial Intelligence's Sticky Wicket*, Iowa Law Review (forthcoming, 2021).
[62] *Id.*

data are both necessary and at least partially identifiable due to the necessity of these devices to deliver personalized medicine.[63] Data essentialism, though, actually risks exploiting the very patients the health care sector is designed to help: when data are absolutely required for medical devices to function safely and efficaciously, and data are necessary for AI development, more than just financial profit spurs ubiquitous data collection.

A. Personal Information in Medical Device AI

While the medical potential is great, these data exist solely because an organization surreptitiously collects, records, and uses data through a human being's technology use and bodily function. Without natural, biological human use and the presence of a human body, these devices would not function to their potential, whether such data are collected during clinical trials or after clinical trials when the medical device is in commercialized use.[64]

Human-computer *collaboration*, as coined by Dr. Krista Kennedy, elaborates this symbiotic relationship: as much or more than individuals need technology, technologies need humans to provide data.[65] Despite the disembodiment of data once data are collected and stored on remote servers, these data exist in relation to the individual,[66] whether produced because of the human-computer interface or supplied from an independent source, such as medical records and medical imaging.

Medical devices using AI may be commercialized for broad use in locked or unlocked format. Locked algorithms are locked at the point of FDA submission and have been created based on the data humans have already supplied through their use in clinical trials.[67] Unlocked algorithms continuously adapt based on real-time device use.[68] Even when devices are used in "locked" format, the predominant type of AI the FDA has approved, human-device data is collected after commercialization to update the algorithms for a new release of the product.[69]

Overall, data collected through human use of a device (as in implantable or wearable devices) or via use of a device on a human (as in surgical or diagnostic technologies) are tremendously important for device safety,

---

[63] *See* supra note 61.
[64] *See* Tschider, supra note 31.
[65] *See* Krista Kennedy, *Designing for Human-Machine Collaboration: Smart Hearing Aids as Wearable Technologies,* 5(4) COMM. DESIGN QTRLY 40 (Dec. 2017).
[66] *See* supra note 6.
[67] US FDA Artificial Intelligence and Machine Learning Discussion Paper
[68] *See* Tschider, supra note 31, at 1572-73.
[69] *See* Tschider, supra note 61.

efficacy, and overall innovation, as are data supplied through external data stores.[70] This model might not cause much concern given its criticality for safety and effectiveness, but the nature of which data are used, how data are used, and how algorithms actually make decisions (that will affect device functionality) are largely opaque as Frank Pasquale, Danielle Citron, Nicholson Price, and Arti Rai have explained.[71]

Organizations purposefully keep these practices confidential or secret and technologically—advanced algorithms may not be readable even by their creators.[72] The combination of both technical opacity and continuous changeability of such algorithms can be described as dynamic inscrutability.[73] Dynamic inscrutability dramatically reduces the likelihood of effectively providing transparency of how decisions in AI are made.[74]

B. Health Data's Inherent Exceptionality

AI technology aside, the necessity of big data foundations for AI challenges traditional notions of the typical medical exchange: personal information supplied to receive medical services. In "small data" exchanges as in traditional medicine, the players are well-known and the formats and systems containing such data reasonably expected.[75] For example, in small data implementations prior to passage of the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, most health information was captured in paper health records.[76] The passage of HITECH and later, the 21st Century Cures Act, served to modernize health transactions, including the portability of medical records between providers and submission of electronic insurance claims.[77]

Under the 1996 Health Insurance Portability and Accountability Act (HIPAA) and subsequent updates of the Privacy, Security, and Data

---

[70] *See* Tschider, supra note 31, at 1572 n.98.
[71] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 6-7 (Harvard U. Press: 2015); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 10 (2014), https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4796&context=wlr; W. Nicholson Price II, *Black-Box Medicine*, 28 HARV. J. L & TECH. 419, 433 (2015), http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech419.pdf; W. Nicholson Price II & Arti K. Rai, *Clearing Opacity Through Machine Learning*, 106 IOWA L. REV. 775 (2021);
[72] Charlotte A. Tschider, *Beyond the "Black Box,"* 98 DENV. L. REV. 683, 685 (2021), https://static1.squarespace.com/static/5cb79f7efd6793296c0eb738/t/60d3e0bf9747b21534fc25d1/1624498369073/Vol.98_Issue3_Tschider_APPROVED.pdf
[73] *Id.*, at 718.
[74] *Id.*
[75] *See* infra note 85.
[76] Gabby Marquez, *The history of electronic health records (EHRs)*, ELATION BLOG (Aug. 4, 2017), https://www.elationhealth.com/blog/history-ehrs/.
[77] Modernizing Public Health Data Systems: Lessons From the Health Information Technology for Economic and Clinical Health (HITECH) Act | Health Care Reform | JAMA | JAMA Network

Breach Notification Rules from 2001-2003, Congress (albeit indirectly) aimed to protect the privacy of individuals seeking services from providers and payment from insurers.[78] The passage of HIPAA and its later modernization efforts laid a path for protecting patient privacy while modernizing the healthcare experience for the benefit of patients and ease and efficiency for all parties involved.[79] When HIPAA was first enacted, Congress could not have anticipated the ways in which electronic data might be used by a myriad of entities, including not only covered entities as defined under HIPAA and their business associates.

And yet, Congress did not pass a generally applicable privacy law as the European Union and several other countries in the European Economic Area had done just two years later in 1998. Instead, Congress took the approach of passing sectoral laws, or laws that focused on sectors and populations where greater risks could exist: health, education, finance, investment, and marketing activities.[80] Other laws focused on specific types of data, such as video rental, electronic communications, credit information, and children's data.[81]

A significant motivation for passing these laws was recognition that these sectors and data were sufficiently and inherently important, that data misuse could result in a variety of harms to individuals, and that a lack of compliance with specified practices demonstrates harm or risk of harm. Such harm or risk of harm may be grounds for enforcement, including statutorily defined fines, *even if* the action itself does not result in data misuse or other generally recognized legal injuries, like financial impacts or job loss.

These laws had something important in common: the requirement of communicating a privacy notice (or privacy policy) specifying planned uses, actually restricting data use to disclosed uses and, in the case of HIPAA, a general requirement of data *minimization*. It is important to consider why notifying individuals about data collection and requiring minimal collection and use of data was included in these laws at all. If Congress really cared about data misuse, for example, they might have only passed requirements to notify of misuse and levied fines for such misuse or non-protection of data (which was included in HIPAA).

If Congress had simply wanted to reduce the probability of data breaches and subsequent sale of health data, Congress would not have had to pass

---

[78] The original goal of HIPAA was to ensure the portability of insurance from one job to the next, avoiding "job lock" where individuals wouldn't change positions upon concern of losing insurance. The Privacy Rule was adopted in 2003, substantially later after two Administrations' worth of discussion on consent. *See* Tschider, supra note 118.

[79] [Statutory string cite]

[80] String cite [FERPA, GLBA, Reg-SP, TCPA, CAN-SPAM].

[81] String cite VPPA, GINA, ECPA, COPPA, FCRA].

a Privacy Rule at all, focusing instead on HIPAA's Security and Data Breach notification rules. Considering the various rules and requirements together, it seems Congress was trying to do something more: bolster individual choice and individual autonomy with respect to important data through notification of data processing practices.

HIPAA has contemplated data loss and data misuse as injuries in and of themselves by requiring organizations to notify individuals and, in the case of data breaches, to notify the Department of Health and Human Services (HHS). HIPAA also statutorily permits the Office for Civil Rights (OCR), the enforcement arm of the Department of Health and Human Services, discretion in enforcing non-compliance with HIPAA. Although HIPAA does not provide for a right of private action, the existence of the OCR and its ability to enforce HIPAA does illustrate that Congress believed that misuse of data, even misrepresentation of privacy practices in a privacy notice, posed risk to patient autonomy and choice regarding highly personal information.

It is this desire to promote autonomy and choice that is a central function of privacy law overall, not just preventing tangible harms and legally defined injury.[82] And although the U.S. has not established privacy as a civil right like the EEA, the importance of choice (via consent) at the outset of such laws laid the foundation for considering that personal information has some inherent risk warranting additional steps prior to collection.[83] This inherent risk in privacy may be considered deontological, or a risk in and of itself absent some secondary tangible harm, or consequentialist risk, such as financial loss.[84] Part III will discuss these risk types in more detail.

C. Big Health Data's Exceptional Characteristics

Big data implementations, necessary to create all AI products, have dramatically increased the nature of risk for individuals. As Nicolas Terry has explained, health data is exceptional, especially in the big data formats used to supply AI technologies.[85] "Small" data is the data

[82] *See* infra Part III and accompanying notes.
[83] Indeed, it could be argued that not all personal information may carry these potential harms and furthermore, it seems that the *practices* by an organization in a position of power was similarly concerning. Taken together, Congress seems to be concerned about certain practices in relation to statutorily defined sensitive personal information, combined risks of power, exploitation, and injury.
[84] *See* supra note 5.
[85] Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX (2014).

present in medical records, such as a specific pharmaceutical prescription or an illness and medical visit date, data that existed before medical data digitization.[86]

Big data includes much more: device data specific to the individual's treatment or device use, as well as proxies for sensitive data gleaned through big data inferences and supplemental data, as in the Livio's capture of environmental location data or music playlist choices. These data sets may also include cellular location data, data which may be indirectly indicative of health conditions.[87] The primary difference between big data and small data is the size and the degree of inferences, inferences that may nevertheless be able to identify a sensitive characteristic.

For example, dietary data collected in a mobile app for an AdvisorPro insulin pump may be designed to supplement calculations of optimal insulin dosage. However, such data collected over time could suggest, with a high degree of reliability, an individual's religious affiliation or the fact they do have diabetes. Data on eating habits might otherwise seem innocuous and may appear to be non-identifiable, yet data from restaurants or regional staples might nevertheless pinpoint an individual's home location, nationality, work location, or ethnicity. Location data could similarly identify an individual's health condition, such as frequent trips near a dialysis clinic.

Health data, as captured through a combination of small data coupled with additional data can be identifiable, even if steps have been taken to remove sensitive data elements, such as medical device serial number, healthcare visit date, full name, or date of birth. What's more is that such data are *created* by using the device. In the case of Arterys or CyberKnife, the data collected during a diagnostic activity or treatment procedure is necessarily specific to an individual's unique bodily characteristics, such as the shape or condition of tissues or organs.

While these data elements may not be individually sensitive data points, such as an electronic health record number, these data are extensions of the physical body and unique to the individual, as unique as a fingerprint or a retinal scan. Although such data may not independently indicate

---

[86] *Id.*

[87] Location as Health by Anya Prince :: SSRN (forthcoming, 2021).

biological gender or race, often such data are captured in combination with such procedures.

Health data is exceptional not only in its big data form but because of its essential relationship to the human body and relative permanence. Unlike a credit card number that can be changed, data collected through medical records, imaging scans, and medical device use digitally approximate who (at least in part), biologically, physically, and potentially mentally, a person is. Medical devices that technically connect or integrate with external devices, such as mobile devices, frequently include lifestyle and location data that expand this pool significantly.

When data are replicated and shared, even when they are not sensitive, they are data created by a person's interface with a technology and unique to them. Furthermore, AI medical device use is *designed* to be personal: the very reason why AI medical devices are desirable is that they can adapt and learn from an individual's unique characteristics. Without personal bodily data created through human-computer collaboration, AI medical devices would function no better than existing analog and non-AI digital devices.

D. Data Identifiability Risk Mitigation Techniques

If an organization collects a large volume of sensitive data and seeks to promote patient interests, organizations might consider making these data less identifiable, de-sensitization or de-identification. It makes intuitive sense: without data that can identify a natural person, little risk remains; de-identification can reduce the potential for injury to an individual if data are misused. However, big data frustrates accepted de-identification approaches in the U.S.

The Department of Health and Human Services' De-identification Safe Harbor (Safe Harbor), for example, permits organizations regulated under HIPAA to legally use data without restriction, so long as it has been de-identified. The general notion is that de-identified data pose very little risk to a specific patient, so using de-identified data is legitimate, such as using such data for inventive purposes, transferring to partners or affiliates, or selling de-identified big data sets for commercial profit.

Why might an organization do this? Because health data, even de-identified data, are highly desirable for other organizations to expand their big data sets with additional data. For example, insurers typically use data from medical devices to understand device use and efficacy for reimbursement purposes. Other organizations developing medical products may also benefit from access to these data. For AI, (big) data

essentialism means that access to data is not optional for safe and effective AI.

1. De-identification and Anonymization of Big Data

There are two models for de-identifying data under the Safe Harbor: removal of 18 common identifiers in healthcare or expert determination.[88] These 18 identifiers are largely indicative of a small data world, including identifiers that are common in provisioning healthcare, such as date of birth or date of visit.[89] Expert determination requires a third party to apply statistical methods to certify a data set as de-identified and "low risk" to the patient.[90] The de-identification model, however, does not necessarily address the increased risk of identifiability of big data sets.[91]

In contrast, requirements of anonymization, as is the case under EU law, requires an "impossibility of reidentification" standard rather than simply low risk, increasing the standard of protection for individuals.[92] For example, current U.S. law permits pseudonymization, where an organization may maintain fully identifiable data sets for disclosed uses but separate identifiable from non-identifiable data to create two databases. The database containing "non-identifiable" data according to the Safe Harbor, then, can be shared, used without restriction, or sold. The EEA would prohibit this type of solution, as well as increase the threshold for demonstrating a data set can be shared with nearly no risk to the patient.

2. Big Data Identifiability & AI Personalization

The problem with big data, though, is that in reducing risk to the patient through higher standards, data become less useful. Big data sets have been found to introduce greater identifiability due to the ability to create inferences. Inferences are probabilities based on data relationships. For example, de-identified data in enough volume can illustrate patterns that ultimately tell us something personal about the individual. These inferences may be innocuous or justifiably applied if an organization uses them to advance the interests of patients and when such inferences are non-discriminatory.

Realistically, although the Safe Harbor may not adequately protect patients in a big data world, anonymized data probably aren't as useful for AI medical device. Most organizations cannot create functionality and

---

[88] Methods for De-identification of PHI | HHS.gov
[89] *Id.*
[90] *Id.*
[91] Big Data, Big Problems: A Healthcare Perspective - PubMed (nih.gov)
[92] Anonymization | CROS (europa.eu)

useful inferences by permanently removing identifiers. Rather, organizations typically use and maintain full data sets, at least for some period of time; other organizations may create pseudonymized data sets. This means that although risk to patients may be reduced, full, highly identifiable data are located somewhere.

AI medical devices require big health data for safety and efficacy, big data that have been produced through the human-computer interface, rendering data that are highly valuable and necessary to current and ongoing AI functionality and potentially will benefit other organizations. Much of these data, despite applying data de-identification practices, is still identifiable and may be more identifiable when combined with other data sources.

Big data, even in a de-identified state, may introduce proxies for sensitive characteristics about an individual, such as race, ethnicity, disability status, medical diagnosis, religion, sexual orientation, or identity. Although HIPAA and its subsequent updates have laid the groundwork for identifying the unique and inherently risky nature of health data collection, use, and retention, it has not kept pace with contemporary big data and AI practices.

Health data, especially health data used in AI and inferences created by AI, may pose substantial risk to an individual. Datafication, or the process of separating the human from the data, risks data overuse and may ignore data provenance. Overall, efforts to reduce identifiability and, therefore, individual risk, do not work well for AI medical device big data sets as they either give the appearance of low-risk data handling practices (without being low risk) or reduce the usefulness, also reducing safety, effectiveness, and personalization goals.

PART III: PRIVACY RISK AS TECHNOLOGICAL DISCRIMINATION

Privacy laws like HIPAA seek to regulate the industry for the purpose of protecting patients, but *from what harms* should patients be protected? Privacy laws like HIPAA address risk of harm as both inherent, or deontological (harm in and of itself), and consequentialist (the effects of action or inaction). This considerably broad depiction of risk of harm expands our understanding of what "counts" as privacy harm.[93]

[93] There are countless examples of regulating the risk of harm in administrative law generally, and specifically in privacy law. For example, data breach notification laws may include positive legal requirements, but most simply require that an individual be notified if their unencrypted personal information has been subject to a data breach. Notifying is designed to promote self-protection on the part of the affected individual to reduce the degree of harm. However, failing to notify does not, in and of itself, cause any injury – the injury potentially began when a cyberattacker compromised personal information and may have realized its potential when a social security number is used

Privacy harms are usually exploitative in at least some way. Although the term exploitation has several meanings within specific types of law, including elder law, criminal law, and race and the law, exploitation usually means to take unfair advantage of someone, to use someone's vulnerability for one's own benefit.[94] Exploitation may be transactional or structural, in that unfairness may be based on a discrete relationships or endemic to the entire system.[95] At some point, the degree of unfairness may exceed our normative accepted values as a society, and what was initially unfair but acceptable may have become discriminatory with respect to a defined group.

For example, a privacy harm may be exploitative in that personal information is directly bought and sold, then used to directly harm someone or for independent commercial gain with no corresponding benefit to the individual. But exploitation also results from the extensive collective exposure of patients to commercial surveillance, often within disproportionate relationships of power that leave patients with few choices. As Mark Andrejevic explains:

> For both legal and regulatory purposes, the notion of privacy, narrowly construed is insufficient for the task of thinking about the pressing issues surrounding information collection and use . . . Like labor power in the industrial era, personal privacy is something that individuals surrender in exchange for access to resources – and they do so under structured power relations that render the notion of free or autonomous consent at best problematic.[96]

Exploitative behaviors might be motivated by desire to collect data about a community where data are highly desirable, such as from people of color or people who have immigrated to the United States. Exploitative behaviors might also be motivated by relationships where the individual has little choice, except to walk away from coverage altogether, such as when they are reliant on government assistance, or even when receiving employer-provided insurance. Exploitation, as explained below, may also result within and alongside certain relationships of trust.

Not all exploitation is harmful: some exploitation can be mutually beneficial, leaving both parties better off, though typically these forms of exploitation disproportionately benefit the commercial party.[97] But

---

illegally to request a bank loan. The behavior of the notifying organization is not directly connected to the injury at all—yet it may affect the degree of injury downstream.

[94] Exploitation (Stanford Encyclopedia of Philosophy).

[95] *Id.*

[96] Privacy, Exploitation and the Digital Enclosure by Mark Andre jevic :: SSRN, at 47.

[97] *Id.*

exploitation is usually harmful, at least in part, to one party while being beneficial to the other. Although exploitative practices are common in surveillance capitalism generally, technological discrimination likely results when exploitative and self-dealing practices exceed benefits to the patient.[98]

A. Deontological and Consequentialist Risks and Privacy Harm

To understand how an individual may be exploited, it is important to first understand how exploitation can occur and to what degree privacy laws prohibit it. Capitalistic exploitation is central to capitalism, the social frame for information collection and use in the AI medical device business community. But regardless of this social frame, exploitation often is indicated by asymmetrical exchanges, and its relative, expropriation, occurs from direct confiscation of resources without confiscation within the exchange.[99] Although it's possible that data and money exchanged for products or services *may* be symmetrically exchanged, it is far more likely that both the exchange and the underlying power relationships are coercive, whether due to information symmetries or power differentials.[100]

When determining what statutory privacy requirements (if any) should apply to organizations engaging in certain activities, such as collecting personal information, legislators discuss statutory provisions reflecting both *risk*, or the potential for harm, and *injury*, legally defined harm. Risk of harm informs how legislators determine what to prohibit and to require in a statutory framework, *ex ante*. Injury is actual impact to individuals, impact that is usually defined in statute to establish injury as part of a prima facie case requirement, depending on the cause of action (usually negligence per se), *ex post*.

Ex ante statutory frameworks generally aim to reduce risk of harm by creating compliance models where administrative agencies, such as the Department of Health & Human Services' HIPAA enforcement arm, the Office for Civil Rights, then enforce compliance with the law. Some non-compliance may also be harm in and of itself, drawing upon deontological risk.

---

[98] Exploitation is typically framed as connected to commercial activities, as in labor generation, and was largely criticized by Karl Marx. Although it could be argued that simply using a medical device or producing data through living is not "labor," data have substantial commercial value, especially for AI medical devices. *See* supra note 11 (describing the medical industry cases where substantial income is made).

[99] MARIANO ZUCKERFELD, *Capitalist Exploitation,* KNOWLEDGE IN THE AGE OF DIGITAL CAPITALISM 122 (Westminster: 2017).

[100] *See* supra note 96, at 48.

1. Risk v. Harm and Risk as Harm

Defining risks and harm is crucial because *some* risks and anticipated harms do not result in statutorily defined injuries—they are harms in and of themselves that result from non-compliance. Non-compliance *is* the harm and may be fineable by an administrative body, such as OCR or the Federal Trade Commission. In privacy law, these types of risks, where harm is inherent in the action, are considered deontological and the harm may be dignitary in nature when the action or omission is directed at an individual.[101]

Risk occurs when it is possible but not certain that some undesirable event will occur.[102] In information privacy and cybersecurity contexts, risk is usually approximated by the probability of some undesirable event occurring and the impact when the event occurs.[103] These descriptions of risk, however, fail to account for the intangible nature of inherent risks to an individual's autonomy, such as processing of data without an individual's knowledge or opaque AI decisional processes.

2. Legally Recoverable Injury Standards

In discussions of morals and ethics, a common debate includes whether ethical and moral obligations result from deontological or consequentialist theories of justice.[104] Consequentialist theories define "moral rightness exclusively in terms of what produces the best consequences."[105] In this model, only consequences of an act are considered, not the act in and of itself. Consequentialist theories map well to common law conceptions of injury under Article III requirements for standing—in particular, that to proceed in a federal lawsuit, injury must be non-speculative or future in nature, and that claims of injury must be sufficiently definite.[106]

The evolution of Article III requirements, especially for privacy law, is one of ongoing debate, and recent court decisions such as *Spokeo, Inc. v. Robins* (2016) have, to some degree signaled muddiness in what legally

---

[101] In privacy law, dignitary harm is typically reserved in privacy law for "invasions of privacy," torts that have a physical component to them, such as placing a Web Camera in a person's private residence, where no independent injury occurs outside the loss of privacy itself (e.g. privacy of intimate relations or the unclothed body, based on the internal sanctity of the home). However, statutory harm for privacy statutes—non-compliance actions—functions much the same: it is harm because *we* say it is, and usually these harms would not be recognized at the common law.

[102] Risk (Stanford Encyclopedia of Philosophy)

[103] CHARLOTTE A. TSCHIDER, INTERNATIONAL CYBERSECURITY AND PRIVACY LAW IN PRACTICE (Wolters Kluwer: 2018).

[104] Jonathan Quong, *Consequentialism, Deontology, and Distributive Justice*, OXFORD HANDBOOK DISTRIBUTIVE JUSTICE.

[105] *Id.*

[106] Rizzo v. Goode, 423 U.S. 362, 372 (1976); *Laird v. Tatum,* 408 U.S. 1, 14–15 (1972).

recoverable injury meeting Article III really means.[107] Indeed, the U.S. Supreme Court reiterated that a pure procedural violation may not be recoverable under Article III, and that injury must "actually exist" or there must be a "risk of real harm."[108]

In *Spokeo*, the Court illustrated that definiteness may actually be the measuring stick for whether plaintiffs may recover. Even if injury could be in the future, it must be reasonably certain to occur and relatively specific as to what the injury would be. The nature of data loss and misuse generally does not easily fit with this very limiting perspective, and, as described in this part, harms could look very different than the Court may expect.[109] That said, district courts have begun to identify injury in data breach contexts more expansively over the past three years.[110]

3. Expanding Views of Risk

Deontological theories of justice define actions as good in and of themselves with respect to the individual and, for example, duties they may be owed. Deontological theories reject other concepts of good action where that action benefits some while reducing benefit to others, such as utilitarian theories of justice, where collective benefit weighs over individual rights.[111] Deontological theories are not mutually exclusive to consequentialist theories, necessarily, and indeed although an overall theory might direct towards a way of measuring rightness or wrongness, under statutory regimes, deontological and consequentialist theories of justice may be complementary.

For example, strict liability statutes like those establishing speed limits arguably have nothing to do with the actual result of speeding. Rather, the collective risk of speeding increases risk to other drivers, pedestrians, and property owners. Speeding, from the perspective of state law, is inherently dangerous. Other strict liability statutes for inherently dangerous activities such as detonation of explosives in construction similarly punish under strict liability, though these statutes are only

---

[107] 578 U.S. ___, No. 13–1339, slip op. at 8–10 (2016).
[108] *Id*.
[109] Daniel Solove & Danielle Keats Citron, *Risk and Anxiety A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 740 (2018), Risk and Anxiety | Texas Law Review. As Solove and Keats Citron explain, the Court in *Clapper v. Amnesty International USA* reiterated that standing requires "injury that is concrete, particularized, and actual or imminent (as opposed to hypothetically possible)." Indeed, the plaintiffs could not show proof that injury was imminent. The Court continued to explain that "in some instances . . . substantial risk that the harm will occur" would be sufficient. *Id.*, at 741 n.14.
[110] Charlotte A. Tschider, *An Empirical Study of Data Breaches* (forthcoming, 2022); Felix T. Wu, How Privacy Distorted Standing Law (depaul.edu).
[111] *See* supra note 104.

triggered when some injury is experienced—they simply short-cut a need to show proximate cause in a tort lawsuit.[112]

4. Privacy Harms and Administrative Law

Privacy harms, broadly construed, illustrate both deontological and consequentialist risks and corresponding harms. These harms may also be measured from an aggregate harm perspective. For example, the Federal Trade Commission, arguably the primary broad administrative agency enforcing privacy commitments under Section 5's broad "unfair or deceptive trade practices," has found success framing harms from a consumer market perspective. For the consumer marketplace, providing incorrect and, sometimes, incomplete information in a privacy notice (with respect to actual data processing activities) may chill consumer behavior and hurt consumers collectively. Of course, this model is more utilitarian in nature, measuring harm from the perspective of the collective benefit or injury of the whole, but it is distinct from the type of injury identified under Article III.

Other enforcement agencies, like the OCR, are statutorily permitted to enforce statutes like HIPAA, which arguably contain steps statutorily defined organizations must take to reduce risk to individuals, such as minimizing data collection, use, and retention or implementing security controls. Such an approach is more reflective of deontological theories, since fines may be levied for non-compliance, though often injury is illustrated again from the perspective of the collective rather than an individual patient, an economic type of harm. Although administrative agencies arguably are defining a pseudo-common law approach with their body of consent decrees and orders, this body of law is private in nature: decrees and orders are private settlements between the agency and organizations, settlements that are not precedential in nature.[113]

---

[112] The difficulty of establishing standing has motivated some scholars, especially those in cybersecurity law, to argue for strict liability for data breaches. Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches,* 127 YALE L. J. 614 (2018), The Yale Law Journal - Forum: Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches; James C. Cooper & Bruce H. Kobayashi, *Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem*, Mich. Tech. L. Rev. (forthcoming, 2021), Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem by James C. Cooper, Bruce H. Kobayashi :: SSRN; Mark Geistfeld, *Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability*, 66 DEPAUL L. REV. 385 (2021), Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability by Mark Geistfeld :: SSRN.

[113] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy* Microsoft Word - S&H 4.3 (stanford.edu) (exploring the nature of FTC action and consistency in FTC consent orders to develop a kind of pseudo-common law); *c.f.* Justin (Gus) Hurwitz, *Privacy, Security, and the FTC's UnCommon Law*, Hurwitz_Gus.pdf (berkeley.edu) (describing the key differences between administrative agency behavior and common law in courts).

Common law tort and private contracting illustrate injury from a consequentialist perspective. In common law tort, such as negligence, injury must be demonstrated either to state standards of injury (in the case of state adjudication) or to Article III requirements as defined by the Court. Typically, injuries are framed as the impairment, or setback of an individual's interests, in short, if the individuals is in worse shape than prior to the harm occurring.[114] In negligence per se actions, courts often find more flexibility in recognizing injury because the statute likely specifies what recoverable injuries are, whether statutory non-compliance or specifically defined. Courts find contractual injury based on what the parties have privately defined as valuable and how material such terms are, or material breach. No matter the measuring stick, the common law often adopts a consequentialist approach to risk and harm.

B. Risk and Statutory Obligations to Avoid and Transcend Risk

Much of privacy law deals in the language of risk: statutes are designed to reduce risk to the individual. Medical device regulation similarly seeks to reduce risk, just from a safety rather than a privacy risk perspective. Neither of these statutory landscapes expect perfection. Indeed, the expectation is one of *reasonableness* and good-faith effort, in large part.[115] Compliance functions within organizations similarly note non-compliance or partial compliance with a statutory requirement as "risk," or risk of harm, whether such harm is inherent or consequential.

1. Defining Risk of Harm

In privacy law, consequentialist risks of harm are focused on the harm: the harm may be actual monetary losses, job loss, or denial of entitlements or other services that results from a data breach, data misuse, or discriminatory intent.

Deontological risks are tied to inherent harms, such as overcollection or overuse of personal information. They may also include risks that increase the combined probability of consequentialist risks, such as excessive data collection that could expose an individual to greater likelihood of a cyberattack or insurance fraud. Therefore, there are three discrete types of risk (*see* Table 1).

---

[114] *See* supra note 109, at 747.

[115] For tort, such practices must be reasonably foreseeable, and such foreseeability is either construed based on reasonable duties that are expected to be owed to another party or, as under negligence per se, when published statutorily providing a private right of action.

Risk Type	Description	Harm
Deontological	Risks that are risks not because they lead to harm but because the risk is the harm itself	Risk is the harm, usually to autonomy (Deontological harm)
		Risks do not lead to harm directly but broadly increase the likelihood of harm generally (Meta-deontological harm)
Consequentialist	Risks that lead to defined harm	Harms are typically identified in existing jurisprudence (monetary loss, loss of job, loss of housing, physical injury)
Utilitarian	Risks that lead to broadly applicable harms, harms that are not outweighed by benefits to society	Harms are to broad structures designed as "good," as in consumer confidence or economic value across organizations or community groups

Risks are mitigated by a combination of proscriptive actions an organization must take with an individual's opportunity to agree to practices that might otherwise be excessive. In application, privacy laws include both *ex ante* requirements, such as conducting risk assessments, with mandated steps that include some private law, like displaying a privacy notice and requesting consent to it. Analyzing these two scenarios, not conducting security risk assessments increases the probability that individuals will experience a data breach. If later a data breach does occur, is the failure to conduct a risk assessment the cause of the injury? Or did it collectively increase risk to everyone?

2. Risk of Harm in Private Law (Contract)

Private law might operate differently. A privacy notice may specify certain commitments made. When an organization deviates from these commitments, two types of risk could hypothetically occur: deontological risk because an organization misrepresented their practices harming individual autonomy. For example, if a medical device manufacturer desired to use data to create a new and innovative device, the manufacturer could explain these additional uses and solicit consent from the patient. Notice and consent are used to expand the collection and use of data beyond what a patient might expect, attempting to strike a

balance between individual interests and commercial interests, negotiated through a quasi-contract (the privacy notice and terms of use).

The challenge, however, is that notice and consent, procedures used to overcome any risks associated with excessive data collection and use, are imperfect substitutes for choice and therefore cannot eliminate deontological risk.[116] Indeed, big data infrastructures destroy previously defined, reliable processes like informed consent in clinical trials.[117]

As Daniel Solove, Neil Richards and Woodrow Hartzog, and this Author have explained, consent is an imperfect substitute for meaningful choice, at least if the law values individual autonomy.[118] Helen Nissenbaum has described the importance of autonomy in relational constructs, reminding us that autonomy can inform choice when "guided by principles . . . adopted a result of critical reflection."[119] Indeed, the effectiveness of consent as choice, and choice in general, is informed by the degree to which human autonomy is diminished in the process. It cannot alone overcome deontological risk.

Private quasi-contracts in the form of a Privacy Notice are usually required under privacy laws. Public drafters of privacy legislation seem to expect notice and consent to overcome bad practices—affected individuals have the power to refuse detrimental practices after reviewing the privacy notice and seek other products or services.[120] However, privacy notices coupled with consent do not cure imprecise and non-salient language that apprises an individual of actual risk, and the sheer number of privacy notices presented to individuals makes it nearly impossible to read all of them anyway.[121] Privacy notices have largely evolved to be exercises that protect the organization from liability rather than actually inform individuals of risk to them.

HIPAA requires disclosure of planned data use related to treatment, payment, and healthcare operations in the notice of privacy practices, and a HIPAA privacy authorization requires even more specificity in uses and the duration of such uses. Unfortunately, the disclosure model itself is

---

[116] Indeed, the concept consent as a complete defense to any number of torts is well-known. Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth* 22 N.C. J. LAW & TECH. 617 (2021).
[117] Michael Froomkin, *Big Data: Destroyer of Informed Consent*, 27 YALE J.L. & TECH. 27 (2019).
[118] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019); Charlotte A. Tschider [hereinafter, Tschider], *The Consent Myth: Improving Choice for Patients of the Future*, 96 WASH. U. L. REV. 1505 (2019); Charlotte A. Tschider [hereinafter, Tschider 3], *AI's Legitimate Interest*, HOUST. J. HEALTH L. & POL'Y (forthcoming, 2021).
[119] Helen Nissenbaum, *Privacy as Contextual Inquiry*, 79 WASH. L. REV. 119, 124 (2004).
[120] *See* Richards & Hartzog, supra note 118.
[121] M. Ryan Calo, *Against Notice Skepticism*, 87 NOTRE DAME L. REV. 1027, 1065-67 (2021); *see* Tschider 1, supra note 118, at 1520-26 (describing voluntariness, structural, cognition, exogeneity, and temporal problems).

broken because it depends on a patient to walk away if they do not agree with the disclosed uses.

To be fair, privacy laws like HIPAA do require additional protective steps, such as adhering to the Security Rule, notifying patients of data breaches and unauthorized use, and permitting patients to revoke consent in addition to other data subject rights. However, these protections are largely procedural, or performative,[122] and do not address the underlying exploitative issues in health technology: power, trust, and opacity. In short, privacy laws today are written from deontological, utilitarian, and consequentialist approaches to individual risk and harm. However, such laws ignore the collective underlying structures of relationships and technologies, structures that dramatically increase privacy risk and degree of privacy harm to specific groups.

Despite Congress' *desire* to motivate individual autonomy through choice and avoid paternalistic governmental interference in private relationships, current privacy models build on rotten scaffolding, adhesive and usually patently unfair scaffolding that ignores substantial power dynamics and commercial interests that lead to exploitation. These dynamics are always present for consumers generally but are significantly more problematic and exploitative in healthcare due to 1) the exceptional nature of healthcare data (as described in Parts I and II), 2) the power dynamics and existing fiduciary relationships present in healthcare relationships and specifically for AI technologies, and 3) the opaque nature of AI medical products.

C. Relational Trust and "False Trust"

As scholars such as Neil Richards, Woodrow Hartzog, and Ari Waldman have explained in great detail, trust is essential in any relationship, including relationships between organizations and individuals.[123] Richards and Hartzog, for example, have noted that trust-based relationships may prove useful in defining how information relationships *could* work and evolving the nature of these relationships based on their context.[124] Indeed, a relational conception of privacy is needed to better understand our commitments to each other, relationships that consider "what powerful parties owe to vulnerable parties."[125]

---

[122] SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS (Cambridge: 2021)
[123] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 447 (2016); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. (2021, forthcoming); *see generally,* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (Cambridge Univ. Press: 2018).
[124] *See Taking Trust Seriously in Privacy Law*, supra note 123, at 457.
[125] Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?* 4 EPDL 1, 2 (2020), A Relational Turn for Data Protection? by Neil M. Richards, Woodrow Hartzog :: SSRN.

1. Trust Intermediaries

Improving these relationships is a challenge, as largely human-to-human relationships of trust have been replaced by human-computer interfaces.[126] Today's "trust," even in healthcare, is often created through one-way communication from the organization to the individual with quasi-contractual notices and an organization's actions consistent with those notices. There is no meaningful opportunity for feedback. More contemporary notions of trust in these relationships include providing individuals with the ability to act on their own interests via design factors that permit an individual to granularly make decisions about their information, such as discrete and modular privacy preferences.[127]

2. False Trust

AI medical devices present a more complex problem: *false trust*. Although enhancing trust should be a central goal of all relationships that involve privacy, it is precisely the existence *of* a trust-based relationship in healthcare AI technology that complicates goals of greater trust. Specifically, false trust results from the essential nature of a high degree of trust in healthcare relationships, a preexisting fiduciary relationship that cannot perform its function, a false fiduciary relationship present in human-machine collaborative relationships, and a lack of available information due to legal and technical opacity that could otherwise enhance trust.

Ultimately, the existence of a fiduciary relationship in healthcare complicates trust surrounding the use of AI medical devices. Under the law, usually under statute and under contract, medical fiduciary relationships are established. The law narrowly defines fiduciary relationships to enumerated persons and situations where a "special relationship of trust" exists. Statutes define fiduciaries in this way because fiduciaries are expected to perform their duties on an ongoing basis, sometimes even after the relationship has ended.[128] The goal in a fiduciary relationship is to prevent injuries from occurring, injuries that result from fiduciaries acting in their own interest rather than the

---

[126] *See The Consent Myth*, supra note 80, at 1512. The replacement of individual trust relationships, where discussions might be conducted in-person with a human being, with form privacy notices, has not buoyed crucial relationships of trust. *Id*.

[127] WOODROW HARTZOG, PRIVACY'S BLUEPRINT (HARV. U. PRESS: 2018).

[128] One exception does apply in tort law, but this only applies when injury occurs: the undertaker's duty. The undertaker's duty applies when an individual takes some positive action for another in such a way that prevents or dissuades others from taking that action. Classically, it's applied when a person visually needs aid: for example if a restaurant patron is choking and someone walks toward them to give help, it is expected the other person will, in fact, try to help them. If they do not, the person could have received help from someone else.

individual's, often called a duty of loyalty and, in the case of physicians, a duty of care.

The goal of narrowly defining such relationships is two-fold: to put individuals on notice where their position of power, and of trust, will result in reliance on them, and second, to determine when additional duties may be expected of them. For example, a doctor's recommendation for a patient to use a medication for a purpose not indicated on the label will likely be viewed differently than a manufacturer recommending the same thing.[129]

Although patients are beginning to act on their own behalf, doctors stand in a position of expertise—and hold themselves out as such—receiving many years of training to become medical experts. Broadly requiring non-medical experts to perform the exact same duties probably does not make sense:[130] we expect individuals to look out for their best interests generally, rather than believe anyone they might encounter.

3. Fiduciary Relationships

Fiduciary relationships also exist because there is inherently greater risk associated with the activities between a fiduciary and an individual. For example, the same doctor recommending a patient take an experimental drug for which they are receiving financial incentives may be breaching their duty of loyalty, resulting in the patient being injured (a treatment paid for by the patient, their insurer, or the government). When a fiduciary gets it wrong, there are far greater impacts for the individual.

Moreover, fiduciary relationships exist because we, as a society, *want* people to trust fiduciaries. It is good for society, and for the economy, for patients to trust their doctors, for customers to trust their banks, for clients to trust their attorneys. The presence of fiduciary relationships gives everyone greater confidence in the system, greasing the wheels of any number of commercial relationships and information disclosures.[131] And, perhaps optimistically, society also cares about individual autonomy. Individuals should be able to make informed decisions in their best interests, relying on experts to help them.

---

[129] The concepts of medical malpractice and products liability are two distinct areas of tort law for a reason, usually because the existence of a fiduciary relationship changes the nature of the duties and the harm.

[130] *See* infra Part IV and accompanying notes. Broadly applicable fiduciary duties could be recognized in limited circumstances where risk is high, trust necessary, and specialized expertise needed.

[131] It should be noted that many members of American society do not view healthcare professionals as individuals to be trusted, given the history of abuse in specific communities. For these communities, trust is not preexisting—it has yet to be built despite the existence of statutorily defined duties.

In healthcare, fiduciary relationships are connected to three central duties: confidentiality (keeping private details confidential), loyalty (acting in the patient's best interest), and care (choosing the best course of action for an individual patient to heal rather than harm). Healthcare is a complex field, and doctors provide a substantial amount of guidance and action—from diagnosing a patient to offering treatment options to directly treating the patient. Any erosion of trust poses significant risks to not only the field of healthcare but also human health.

In AI healthcare, however, nearly all of these activities are either performed by a manufacturer's device or with a manufacturer's device. However, manufacturers are not currently fiduciaries though arguably they benefit from existing fiduciary relationships. The creators of AI technologies are often not members of the healthcare community at all (or regulated as such).[132] Start-ups, for example, survive through commercialization of a product; the goal is to sell it. In healthcare, these organizations are often acquired by a larger medical device manufacturer that does not have the expertise to create the AI. In some cases, AI technology developers create AI platforms that can then be licensed to medical device manufacturers to create or integrate products.

And, although manufacturers may not be "manipulating trust" outright, they benefit from false trust.[133] While trust exists between physicians and their patients, and physicians do not often understand how AI medical devices work, and medical device manufacturers may not even understand how the AI works. If patients are dependent on their doctor for information about privacy practices, the doctor is ill-prepared to answer them; perhaps even more worrisome is a lack of concern about privacy practices, because the presence of fiduciary relationship creates a false sense of security.

D. The Choice Paradox: Your Privacy or Your Life?[134]

In the event a patient desires to influence their privacy interests, they are faced with an impossible choice: do I follow my doctor's orders and live (or improve my quality of life or health outcomes) or choose privacy? Choice in this respect is not a matter of whether or not to consent to a

---

[132] Start-ups, Amazon, Google, IBM, etc.

[133] Usually issues with trust are described as intentional manipulation. *See* Waldman, supra note 123, at 92. However, the existence of alternative, ineffective trust is a different concern.

[134] Ari Ezra Waldman describes the "Privacy Paradox" wherein individuals care about privacy but do not make decisions in line with these interests. I use the terminology of "Paradox" here to describe a kind of super-adhesive contracting and relationship—although it may *appear* as if a patient has a choice, the patient actually has no reasonable choice. In these scenarios, a patient must choose between life, or quality of life, and privacy, a Hobson's Choice for healthcare.

privacy notice but whether or not to use AI medical device technology at all, a concept inherent in adhesive contracting generally.

Choosing to walk away from a comparatively more safe and efficacious surgical procedure is not the same as choosing an alternative coffee maker. The stakes are much higher and indeed, the available alternative options may be fewer. Ultimately, privacy law as it stands is not equipped to tackle the dynamic environment created by AI, primarily framed to focus on individual rights and "choice."[135]
Modern economics, owing much to Vilfredo Pareto, often describes consumer behavior as ranked preferences, or ordinal utility, listing preferences in order with respect to each other.[136] In privacy law, this likely means that there may be preferences that rank higher than privacy interests, for example incentives to exchange data for cash payments, coupons, or better technology offerings. However, in healthcare, these interests are more nebulous. Consider the following scenario:

> *Angel, a privately insured patient with a moderate income who has classically had a strong relationship with the healthcare system, needs an insulin pump to manage their Type-1 diabetes. Angel is presented with two options by her doctor, both insulin pumps that use AI systems. Angel knows that AI collects a lot of data – after-all, the pump connects to their mobile device and provides reports to their doctor.*

Even if Angel cares about their privacy and receives accurate information about how their data will be used, it will probably not be enough to forego using the pump or deviate from their doctor's recommendation. Assuming no other considerations go into the decision, such as how much their insurance will pay, Angel will likely proceed. In this scenario, Angel does not really have meaningful choice because the context of making the choice cannot overcome inherent ranked preferences of the healthcare environment.

Angel's life experiences, however, could radically change the outcome of this situation in other negative ways. For example, Angel could be receiving public healthcare assistance, such as Medicaid, and Medicaid requires disclosure of data from the insulin pumps to improve broader

---

[135] *See* supra note 96, at 49.
[136] These preferences are not static: they are animated by community and cultural attitudes and personal experiences. For example, medicine has classically had great difficulty recruiting members of underrepresented communities to clinical trials, despite the potential benefit to these communities, due to a history of exploiting and, in some cases, physically harming people. *See, e.g.*, Tuskegee Experiment: The Infamous Syphilis Study - HISTORY; REBECCA SKLOOT, THE IMMORTAL LIFE OF HENRIETTA LACKS (Crown: 2011); KHIARA M. BRIDGES, CRITICAL RACE THEORY: A PRIMER (Foundation Press: 2018); Leana Wen, *Doctors' Ignorance Stands in Way of Care for the Disabled*, NPR (May 17, 2014), Doctors' Ignorance Is A Barrier To Care For Disabled : Shots - Health News : NPR; KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS (Stanford: 2017); VIRGINIA EUBANKS, AUTOMATING INEQUALITY (Picador: 2018); amongst *many* other examples.

efficiency and quality goals. If Angel does not want their information shared with the government, Angel may have less of a choice because this is the technology Medicaid will reimburse. Or the medical device company could sign a private agreement with Medicaid that arranges for greater data sharing in exchange for a lower device cost.

Angel may also be a member of a community where distrust of the healthcare system is real and the healthcare system has a history of exploiting people like Angel in the community due to their race, immigration status, income level, disability status, intimate affairs, or identity. In this case, Angel may intentionally avoid safer or more efficacious medical device use because the data collected could harm Angel in many other discriminatory ways. Patients like Angel should not have to choose between data use that may pose substantial risk to them in multifaceted ways and safe and efficacious treatment.

In the event medical device choice is not impacted by ranked preference issues, device options may still be comparatively limited. Overall, medical devices are high-innovation technologies protected by patents, and the trade secret and confidential status of the AI they include limits the degree to which competitors can enter the marketplace. Although these devices are designed to solve the most impossible of healthcare issues, they are also not terribly numerous in options. And few devices today boast enhanced privacy protection as a selling point.

E. Inadequate Privacy as Exploitative and Potentially Discriminatory

The cumulative effect of the challenges described thus far is that patients using AI medical devices are very likely to be exploited for their data, data which are highly valuable to an organization. But exploitation is not necessarily discriminatory. Indeed, exploitation may not even be holistically harmful to an individual. Understanding the difference between exploitation and discriminatory practices is essential to determining the appropriate approach to prevent discriminatory practices.

First, it is important to acknowledge that exploitation may be transactional or systemic – exploitation that creates unfairness can be attributed to systemic issues in a sector or cross-sectors. This systemic exploitation is reflected in the underlying prevailing issues of false trust, a lack of similarly efficacious alternatives, and ranked preferences.

Exploitation is likely to be transactional, as well, as organizations rely on procedural privacy fraught with issues, such as notice and consent, and the inability or unwillingness to overcome opacity issues in AI technology and data essentialism. While exploitation stems from

unfairness, the combined impact of substantial systemic and transactional exploitation creates the possibility of discrimination. Discrimination can result from healthcare exploitation when the effect disproportionately affects an individual with respect to their peers, such as having privacy or not having privacy. And, indeed, the way in which an individual is affected may certainly be intersectional in nature.[137]

1. Existing AI Discrimination Concerns

It is well-known that AI can create new discrimination risks based on how data are collected, used, and ultimately decisions rendered. Scholars such as Andrew Selbst and Solon Barocas, Sonia Katyal, Dennis Hirsch, Lilian Edwards and Michael Veale, danah boyd, and Ignacio Cofone have discussed varying AI discrimination problems, including models for resolving issues of transparency and testing to avoid AI issues.[138] However, these descriptions of discrimination fail to explore the context in which these issues arise, the structural exploitation that creates the likelihood of greater discrimination for technology users dependent on medical device manufacturers.

As these scholars have observed, big data has the potential to perpetuate discrimination as currently defined, can encode existing discriminatory impact (including AI training data), or fail to test for unexpected impacts. Because big data feed AI algorithms, such discrimination may be opaque, even to an AI's creators. These issues are not unique to general consumer technologies; they also exist in medical device AI.[139]

Discrimination in this sense could amplify existing issues with respect to predefined protected categories. For example, a patient who could already be exposed to discriminatory risk of harm simply because the patient is a person of color using AI (that may disproportionately affect specific racial groups) may be exposed to even more risk of harm. In this way, technological discrimination works as a multiplier for existing risks.

---

[137] Nancy López & Vivian L. Gadsen, *Health inequities, Social Determinants, and Intersectionality*, NAT'L ACADEMY MED. PERSPECTIVES (Dec. 2016), https://nam.edu/wp-content/uploads/2016/12/Health-Inequities-Social-Determinants-and-Intersectionality.pdf.

[138] Big Data's Disparate Impact by Solon Barocas, Andrew D. Selbst :: SSRN; The Intuitive Appeal of Explainable Machines by Andrew D. Selbst, Solon Barocas :: SSRN; That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority by Dennis D. Hirsch :: SSRN; Private Accountability in the Age of Artificial Intelligence by Sonia Katyal :: SSRN; Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'? by Lilian Edwards, Michael Veale :: SSRN; Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age by Charlotte Tschider :: SSRN; Algorithmic Discrimination Is an Information Problem by Ignacio Cofone :: SSRN; Fairness and Abstraction in Sociotechnical Systems by Andrew D. Selbst, Danah Boyd, Sorelle Friedler, Suresh Venkatasubramanian, Janet Vertesi :: SSRN; Algorithmic Accountability by Alex Rosenblat, Tamara Kneese, Danah Boyd :: SSRN.

[139] *See* Tschider, supra note 31.

2. Technological Discrimination

In addition to predefined groups already exposed to discriminatory risk, patients using compulsory medical devices cannot reasonably avoid risk of deontological harm, creating substantial, and sometimes pervasive, harm. These harms, collectively and deontologically, increase privacy risks to individuals dependent on these devices.

In summary, for these technologies to work safely and efficaciously (as described in Part I), they likely require ubiquitous, continuous, and sensitive data collection, increasing the possibility of direct discrimination or indirect discriminatory impact based on these data elements. From a deontological risk of harm perspective, collectively patients using many AI-enabled medical technologies will be subjected to substantial privacy risk whereas their peers will not. Unchecked, such risks could adversely affect the patients using this technology or could undermine confidence in healthcare AI overall.

In this way, limiting data collection and use is tremendously difficult to achieve because data are essential to AI functionality. The opacity of how AI make decisions with respect to these data further limits how patients can understand how and to what extent their data are used. Finally, when data are disembodied from the individuals creating data through human-computer collaboration, the risk of overuse increases substantially.

3. Fiduciary Duties Foundational to Overcoming Technological Discrimination

The underlying foundation for all relationships, including those involving AI medical devices, requires trust. Patients rely on doctors with whom they have a relationship of trust, but the trust is misplaced when it is inappropriately transmitted to manufacturers and technology providers that are not included within this fiduciary relationship.[140]

The nature of the relationship between a patient and a manufacturer or technology provider *would* be fiduciary in nature if a doctor would be providing the technology or service rather than a third party. The problem, though, is a fiduciary relationship cannot be outsourced, as it is

[140] It should be noted that trust flows both ways. Although we focus primarily on power differentials and the effect on the patient, who is usually vulnerable in the scenarios described, doctors also need to be able to trust their patients. The use of AI technology and its associated surveillance, however, can increase or decrease trust by including more objective data into the picture. In its best case, this objectivity *could* improve doctor-patient relationships, though in others it could erode trust. The scope of two-way relational trust is a topic outside this paper, as it builds on existing fiduciary relationships. *See* 77.full.pdf (bmj.com).

defined statutorily. And in many cases, manufacturers likely would not perform the role of a fiduciary.

When a broadly applicable fiduciary relationship, such as an information fiduciary, *should* attach to a relationship is when the potential risk of harm is significantly high. Otherwise, the role of a fiduciary, especially when other important fiduciary relationships exist, risks losing its importance. When everyone is responsible, no one is responsible. Fiduciary relationships are crucial to the trust of an overall system, and when an individual cannot trust their fiduciary, confidence in system or sector as a whole diminishes.

Moreover, a lack of alternative technologies or equivalently effective technologies forces patients to make choices that deprioritize privacy considerations and increase the potential for misuse. When confronted with a serious health condition, patients will generally choose health rather than privacy.

When all or most of these factors are present, individuals cannot meaningfully protect their data interests, resulting in exploitation that will likely be discriminatory when AI medical device-using patients are exposed to significantly more privacy risk than their peers.[141]

On the balance, risk to individuals reliant on frequent healthcare, or reliant on healthcare technologies, are more exposed than their peers who are not reliant. Most if not all of this healthcare use is compulsory in nature, and there is no real choice possible in whether to provide or not provide data. This collective increased deontological (and, likely, consequentialist) risk creates a disproportionate impact to patients that creates a new kind of discrimination: *technological discrimination*, or discrimination due to technology use, not a predefined status (e.g. race, religion, country of origin, gender identity) exacerbated by it.

PART IV: REDUCING TECHNOLOGICAL DISCRIMINATION

As early as 2001, Ian Kerr proposed that holding information could create some reciprocal responsibility in a fiduciary relationship.[142] The information fiduciary movement calls for the creation of a duty of loyalty for all information collectors. In short form, by collecting personal information, a duty is created. In healthcare fiduciary relationships, a duty of loyalty is not the only relevant duty. For example, a duty of care

[141] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 186-87 (PublicAffairs: 2019).
[142] Ian Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CANADIAN BUS. L. J. 1 (2001).

accompanies duties of loyalty and confidentiality that require a physician to act in the best medical interest of a patient.

In healthcare, an information fiduciary role that acknowledges the realities of a digital world could enhance "dividual privacy" goals.[143] As John Cheney-Lippold describes this new world, we must embrace the new world of privacy while promoting individual interests, as well:

> We need dividual privacy—a privacy that extends beyond our individual bodies, that accepts the realities of ubiquitous surveillance. . . To anoint the individual subject as the sole index of power is to miss out on everything else that happens outside the individual's point of view. . . Understanding that our data is part and parcel of who we are and what we are subject to lets us think about privacy in a new way.[144]

Essentially, dividual privacy creates the *right* incentives and regulatory structures while embracing the realities of legitimate and sometimes beneficial surveillance. AI medical devices differ from general consumer products in that they have the potential to revolutionize medicine for the better, to democratize access, and to even facilitate personalization that improves healthcare equity. Doubling down on failing privacy frameworks will both reduce the safety and efficacy of desperately needed products and services while failing to dismantle the hidden, exploitative, and potentially discriminatory practices of commercial medical device manufacturers and their third parties.

If an information fiduciary role is intended to be effective, a statutorily created role must be sufficiently definite and not replicate existing issues with the current privacy system. In particular, where existing fiduciary relationships exist, the role must be clearly demarcated and not duplicative of known fiduciary relationships, such as doctor-patient or therapist-patient relationships.

Specifically, information fiduciaries should have a positive obligation to illustrate how exploitation of patients, which *will* occur due to the commercial nature of AI medical device sales, does not amount to technological discrimination.

A. Contours of An Information Fiduciary

Jack Balkin resurrected the concept of an information fiduciary in 2016, to varying degrees of support.[145] Balkin's description of the role stemmed

---

[143] JOHN CHENEY-LIPPOLD, WE ARE DATA 236 (NYU: 2017).
[144] *Id.*
[145] viewcontent.cgi (yale.edu).

from data's application to robotics and big data.[146] The three laws reflected the realities of AI and big data, illustrating many of the problems described herein.[147]

First, Balkin described that algorithmic operators are information fiduciaries with respect to their clients and end users.[148] This concept is illustrative of the power dynamics implicit in these relationships: one organization presumably has access to and can control (at least to some degree) how opaque AI systems work and the effect these systems have on individuals.

Factually speaking, certainly this is true, but it could also be argued that this relationship alone would exist for generalized concepts of duty, as in negligence, for example in the undertaker's duty. The undertaker's duty is typically a plaintiff's defense against a defendant's complete defense that no individual has a positive duty to help another. The undertaker's duty applies when a defendant has begun providing assistance, has "undertaken" a duty, which then, if stopped, would leave the individual in a worse position than they started.

There may be scenarios where AI system opacity is innocuous and scenarios where opacity is such a significant problem that a positive fiduciary role is necessary. Moreover, AI may be highly procedural and not likely to inspire confidence or trust. It is highly difficult to distinguish without knowing the context of the situation when a positive duty, as in an information fiduciary, should apply.

Second, Balkin specifies that algorithmic operators have a duty toward the general public.[149] Balkin specifically describes the role of bystanders and other individuals who are not in privity with a manufacturer but who are nevertheless harmed by defective products.[150] Although this concept ties more directly to questions of liability for consequentialist harm, the concept also illustrates the larger environment in which AI systems operate. For example, a loss of trust can result in distrust of the overall system, a system that already is rife with legitimate community-based distrust.[151] The problem is so endemic to healthcare that it is

---

[146] *Id.*
[147] *Id.*
[148] *Id.*, at 1227.
[149] *Id.*, at 1231.
[150] *Id.*, at 1232.
[151] *See, e.g.*, Understanding and Ameliorating Medical Mistrust Among Black Americans | Commonwealth Fund; African Americans and their distrust of the health care system: healthcare for diverse populations - PubMed (nih.gov); Broken trust drives native health disparities | CMAJ; Recognising the historic experience of Aboriginal and Torres Strait Islander patients is key to reconciliation | Australian Healthcare & Hospitals Association (ahha.asn.au); Understanding and Addressing Medical Mistrust | Spotlight Trust™ | The future is trust.; Asian Patients' distrust of western medical care: one perspective - PubMed (nih.gov); Why Many Latinos Dread Going to the Doctor - The Atlantic; HIV status, trust in health care providers, and distrust in the health care system

possible that increasing trust-based relationships where organizations are actually held to their obligations could work to improve the system, *if trust is taken seriously*.

Finally, Balkin relates a third law, that algorithmic operators have a public duty not to engage in algorithmic nuisance.[152] Such algorithmic nuisance is described as engaging in harmful behavior, diffusing harm over an indefinite population.[153] Balkin describes such a nuisance in relation to Andrew Selbst's description of intentionality in algorithmic discrimination: namely, that intent is not the appropriate barometer for discrimination—an algorithmic cannot *intend* to discriminate.[154] Rather, it encodes certain behaviors that render a social effect, and whether such effects are justified.[155]

This concept relates well to the reality of AI medical device exploitation, importantly that exploitation may be endemic to the macroeconomic marketplace and capitalistic dynamics—power differentials and information asymmetries may be unavoidable. However, the *effects*, in particular the combined effects for individuals, communities, and the market overall could justify additional duties on behalf of AI medical device manufacturers.

Frank Pasquale has commented on Balkin's work, importantly adding an additional law of robotics to consider, while cautioning on the third law's applicability.[156] Pasquale specifically describes an "attribution problem," or the challenge of regulating machines without ascribing some legal responsibility to one or many persons, natural or commercial in nature.[157] Indeed, the evolution of AI development could exceed the original creator's intention, and the AI medical device field certain does include both acquiring organizations as well as the potential for continuous learning. These elements mean that the application and scope of fiduciary

---

among Bronx women - PubMed (nih.gov); From Slavery To Present: Why Blacks Distrust Healthcare Pt. 1 | Page 2 of 7 | BlackDoctor.org - Where Wellness & Culture Connect. These articles only begin to scratch the surface of trust issues amongst many U.S. residents.

[152] *See* supra note 145, at 1232.

[153] *Id.*, at 1232-33.

[154] *Id.*, at 1233-34.

[155] *Id.*, at 1234. Pasquale has described the reasonable limitations of a law of nuisance, importantly noting that the well-known nature of discriminatory impact within algorithmic design may result in actual liability in limited circumstances, rather than only a broad social impact. See infra note 156, at 1249. Although this Article does not delve into the details of tort liability for AI, this caution is an important check on unlimited and broad social liability when more specific applications might make sense. This overall caution certainly motivates limiting the application and scenarios in which an information fiduciary role is recognized.

[156] "Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility" by Frank A. Pasquale (umaryland.edu).

[157] *Id.*, at 1252, 1254.

duty could change over time – it is not static but likely flows with the technology itself.

Balkin has expanded the concept further, applying the information fiduciary concept to privacy law.[158] The frame for such an application is very similar to the concepts described in Part III, namely that surveillance capitalism spurs digital dependence, and such dependence requires additional corresponding responsibilities.[159] Balkin succinctly summarizes the broader problem, noting that:

> Although digital companies know a lot about us, we do not know a lot about them—their operations, what kind of data they collect, how they use this data, and who they share it with. Because of this asymmetry of information, we are especially vulnerable to them, and we have to trust that they will not betray our trust or manipulate us.[160]

As Balkin further notes, the issue is not simply asymmetry, it is that digital companies want consumers to use their products, so much of the communication prompts individuals to lean in to technology, to provide more information. As described in relation to the Livio hearing aid, certain technology affordances and ease of use similarly promote reliance and provision of additional data sources, such as the Livio's integration with a mobile device music playlist or health apps.[161] Such devices also direct attention to lifestyle benefits rather than details about how the technology works or the data they collect.[162] The collective impact is that these devices function based on users providing more data, not less.

Finally, in responding to criticism regarding the fiduciary model, Balkin notes that the function of a fiduciary has the potential to overcome broader competition issues.[163] As described in Part III, one underlying competition issue for AI medical devices is the lack of comparable alternatives in the marketplace, as well as forces that direct an individual towards digital devices, such as a physician's standard of care, insurance coverage, or public health assistance, such as Medicaid or Medicare coverage.

These forces, which may have a substantial impact (if a patient opts for a device that is not reimbursable through insurance) along with demonstrated health concerns (creating a sense of exigency in making a

---

[158] 134-Harv.-L.-Rev.-F.-11.pdf (harvardlawreview.org)
[159] *Id.*, at 11.
[160] *Id.*
[161] *See* supra note 58.
[162] *See* supra note 6.
[163] *See* supra note 158, at 21.

decision), outweigh privacy interests when an individual engages in preference ranking.

The information fiduciary model may be broad in nature, but for AI medical devices, this model may be useful. In establishing an information fiduciary role for such manufacturers, however, a critical question is *how* manufacturers can demonstrate duties of loyalty and care with respect to patients, especially when a physician is usually prescribing the device (as in DreaMed AdvisorPro) or using the device in conjunction with the patient (as in surgical robotics like the CyberKnife).

B. How the Information Fiduciary Duty of Loyalty and Care Might Be Demonstrated

Recognizing the role of an information fiduciary acknowledges and names the increased risk to individuals otherwise dependent on healthcare technologies and protects their interests. This section only begins to explore how a fiduciary role could work for AI medical device manufacturers.

As Richards and Hartzog note, where vulnerabilities are low, either because there is currently a small amount of trust or where there is low risk of exposure, duties of care and loyalty might be similarly diminished.[164] However, where vulnerabilities are high, higher duties of care and loyalty might be required.[165] It is precisely this context that reflects the reality of information transactions. In healthcare specifically, scenarios that present a high risk of technological discrimination should demand a greater duty of care and loyalty.

Initially, the information fiduciary role could be narrowly tailored to sectors and scenarios like healthcare, where the deontological (and, potentially, consequentialist) risk of technological discrimination is inherently high. Creating an obligation might be most appropriate at the state level, where fiduciary relationships are largely defined. For example, state healthcare privacy laws could be updated to establish fiduciary obligations in scenarios where AI are used. Such obligations should be published separately and distinguished from general tort obligations which might be preempted under FDA medical device preemption.[166]

---

[164] *See Taking Trust Seriously in Privacy Law*, supra note 123, at 458. Richards & Hartzog propose an alternative description of Discretion, Honesty, Protection, and Loyalty as defining factors for establishing trust in these scenarios.

[165] *Id*.

[166] *See generally*, Tschider, supra note 31 (describing a history of SCOTUS preemption decisions, and the likely and dangerous expansion into medical device AI).

Moreover, the benefit of identifying an information fiduciary role is that harms are reconceived based on duties of loyalty and care. Risk of harm, therefore, including deontological and consequentialist risks of harm, may be sufficient to illustrate when an organization has not effectively performed their duties, rather than the comparatively higher standard of legal injury that applies to common law torts. This model works more effectively for information harms that may be hard to prove. Fiduciary duties, therefore, can be tied to statutorily defined harms, or may be focused on prescriptive duties themselves.

Healthcare privacy laws seem to offer some opportunity for additional responsibilities in this space, as well. First, organizations that are not regulated by HIPAA may now be regulated in some way. Second, organizations that are currently regulated by HIPAA will not be preempted from additional regulation: HIPAA is a floor, not a ceiling, as state healthcare privacy laws demonstrate. Finally, failure to fulfill a fiduciary duty statutorily could be referred to a state attorney general office or similarly construed to demonstrate unfair or deceptive trade practices, which would be similar to how many information practices are enforced today.[167]

Several models could be applied to demonstrate fulfillment of duty. For example, conducting HIPAA risk assessments could count, or increasing salient details in a broadly hosted privacy notice (including identities and locations of third parties, or commercial entanglements) certainly could illustrate some additional duty performance. Other examples could include involving patients in focus groups and feedback sessions on information handling practices.

One of the most powerful activities that an organization can do, however, is to conduct legitimate interest analysis. Legitimate interest analysis explicitly requires organizations engaging in behaviors that substantially increase risk to the patient to identify the interests of the patient, community, or broader public health and the interests of the organization. This assessment might complement other privacy activities but expands the notion of privacy into a model that more broadly concerns dynamics of power and market, and forcing disclosure of commercial benefits. Moreover, when such analyses demonstrate excessive commercial benefit in relation to patient benefit, certain actions could be explicitly barred or enforced by state AGs under a suit involving the breach of a fiduciary duty due to technological discrimination.

---

[167] Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law by Charlotte Tschider :: SSRN; CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (Cambridge: 2016).

CONCLUSION

The advent of AI medical devices brought with it tremendous promise to democratize medicine and improve human health. But it also brought with it a more pervasive and insidious form of commercial exploitation, central to surveillance capitalism. Without an appropriate check on such exploitation, these practices could lead to broader impacts not just to the individual but to community trust in the medical community. By identifying, and prosecuting, technological discrimination by enforcing information fiduciary roles in the AI medical device community, the U.S. can better balance justifiable interests in health data collection and use with the interests of the individual, creating a symbiotic system that benefits all parties, especially patients.