THE CONSENT MYTH: IMPROVING CHOICE FOR PATIENTS OF THE FUTURE

CHARLOTTE A. TSCHIDER*

ABSTRACT

Consent has enjoyed a prominent position in the American privacy system since at least 1970, though historically, consent emerged from traditional notions of tort and contract. Largely because consent has an almost deferential power as a proxy for consumer choice, organizations increasingly use consent as a de facto standard for demonstrating privacy commitments. The Department of Health and Human Services and the Federal Trade Commission have integrated the concept of consent into health care, research, and general commercial activities. However, this de facto standard, while useful in some contexts, does not sufficiently promote individual patient interests within leading health technologies, including the Internet of Health Things and Artificial Intelligence.

Despite consent's prominence in United States law, this Article seeks to understand, more fully, consent's role in modern health applications, then applies a philosophical-legal lens to clearly identify problems with consent in its current use. This Article identifies the principle issues with substituting consent for choice, the "consent myth," a collection of five problems, then proposes principles for addressing these problems in contemporary health technologies.

"In God we trust. All others must bring data." – Unknown[1]

* Charlotte A. Tschider is the Jaharis Faculty Fellow at the DePaul University College of Law. I would like to thank a great many people for helpful comments and suggestions along the way that have improved and guided the development of this article: participants of the Privacy Law Scholars Conference, especially Neil Richards, Daniel Solove, and Gordon Hull; participants of the Internet Works-in-Progress Conference, especially Eric Goldman and Ari Waldman; participants of the AALS Health Law Section Junior Scholar Works in Progress session; participants of the Northern Illinois Junior Scholar Works in Progress Conference; and fellow panelists and commentators at the Washington University Symposium on Privacy & Trust, especially Danielle Citron. I would like to especially thank W. Nicholson Price, Jake Linford, Nicolas Terry, and Fazal Khan for their close readings of this work and substantial comments at various points in its development. I would finally like to thank the DePaul University College of Law faculty for their support and encouragement during the development and substantial revisions of this article and the Jaharis family for their financial support of this fellowship.

1. This quotation is often attributed to W. Edwards Deming, but it is of unknown origin. *See* Barry Popik, *"In God we trust. All others must bring data,"* BIG APPLE BLOG (Oct. 19, 2015), https://www.barrypopik.com/index.php/new_york_city/entry/in_god_we_trust_all_others_must_bring_data/ [https:// perma.cc/3VKS-DLPY].

INTRODUCTION

"Consent" in the privacy context emerged as a mechanism to negotiate the private and public spheres of life. What began as a version of contractual agreement, an affirmative defense in tort, and a precursor to confidential relationships, has grown in digital times to epic proportions. The health industry alone uses at least four different variants of consent: traditional notice with explicit consent, express authorization, informed consent, and notice with recommended consent.[2]

The consent mechanism has subsumed broader conceptions of consumer and patient choice, a concept implicit in broader social goals of autonomy and self-determination. This neglect of broad notions of choice and the synonymous treatment of consent *as* choice has led to a substantially weaker privacy model depending almost entirely on a set of beliefs, or rather myths, that privacy scholars and practitioners have widely acknowledged as longstanding problems. The dominant privacy model today operates almost exclusively by using adhesive privacy notices, followed by agreement to such terms, or consent. So long as the privacy notice is accurate and the natural person about whom data is collected (the data subject) agrees, an organization has met its privacy obligations.

New connected health technologies have amplified these problems, demanding exploration of new privacy models to protect consumer and patient interests. The Internet of Health Things, or Internet-connected consumer health devices, have begun to generate large volumes of useful data, increasing potential data uses. Artificial Intelligence (AI), increasingly used in health applications like disease diagnosis, treatment outcome evaluations, and medical device functionality, requires large data volumes to produce reliable and effective AI algorithms.[3] These technologies, which carry great promise for improving human health, seek to maximize data collection and use, making it more difficult for organizations to effectively communicate information in a privacy notice. The health technology environment has changed rapidly over the past forty years, boosted by Internet-connected resources, faster computing power, shrinking battery size, and transformative power of Internet mobility.[4] However, the pace of

2. It should be noted that this Article examines consent from the perspective of privacy considerations, rather than general patient knowledge with regard to medical procedures and clinical studies, or *informed consent*. There is a wealth of research on informed consent in the medical procedure context, which will not be incorporated here. *See, e.g.*, Nadia N. Sawicki, *Modernizing Informed Consent: Expanding the Boundaries of Materiality* 2016 U. ILL. L. REV. 821 (2016) (describing the limitations of informed consent).

3. *See* Charlotte A. Tschider, *Deus ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future*, 5 SAVANNAH L. REV. 177, 183–84 (2018).

4. Although often these aspects might indicate revolutionary changes to medicine, more likely they will add to existing models (sustaining technologies), rather than operate as technology disrupters.

the law, especially in relation to privacy considerations, has remained fairly static since the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Department of Health and Human Services's (HHS) 2002 Privacy Rule.[5] The Privacy Rule, incorporated by HHS, established patient rights and organizational obligations to be enforced under HIPAA. Despite updates of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), the Privacy Rule has essentially remained the same, as have the Federal Trade Commission privacy principles.[6] The lack of health privacy law updates consistent with the evolution of modern health technology has created incompatible and, to some extent, abusive privacy practices.[7] What may have provided minimally sufficient consumer choice in a traditional health context no longer safeguards consumer privacy interests with modern health technologies.[8]

This Article builds on a bedrock issue raised in Daniel J. Solove's *Privacy Self-Management and the Consent Dilemma*: although consent fulfills certain needs in our privacy system, we are rather expecting consent to do too much,[9] specifically that notice coupled with consent has been positioned as a panacea for nearly all privacy problems. Unfortunately, the consent mechanism is imperfect: although consent may be useful in some scenarios, it does not fulfill greater goals of individual choice implicit in privacy goals. Contextual integrity, however, does provide a helpful tool for evaluating legal schemes, including the normative role consent plays as a functional representation of choice and identifying its considerable limitations, including whether it can, at present, fulfill autonomy goals. This paper adds to the existing privacy literature by applying Helen Nissenbaum's philosophical lens of contextual inquiry to identify and categorize the five primary problems with consent, then proposes an alternative model, as principles, to better support individual choice.

Nicolas P. Terry, *Information Technology's Failure to Disrupt Health Care*, 13 NEV. L. J. 722, 723–24 (2013). Still, the different technology models do, to some extent, frustrate traditional notice and consent models.

5. *See* The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat 1936 (1996); *HIPAA—the Federal Medical Privacy Rule*, CITIZENS' COUNCIL FOR HEALTH FREEDOM (Apr. 2003), http://www.cchfreedom.org/cchf.php/268 [https://perma.cc/BD8U-Y5J8]. The first version of HIPAA required that Congress develop a privacy rule by August 1999. Failing this, HHS would have to draft a privacy rule. *Id.*

6. Although certain aspects of HIPAA were updated via the HITECH Act, these updates mostly expanded obligations to Business Associates, introduced specific data breach notification obligations, and enhanced Office for Civil Rights enforcement powers. Core aspects of privacy notice and authorizations remained. *See infra* Part II.B and accompanying notes.

7. *See infra* Part III and accompanying notes.

8. *See infra* Part III and accompanying notes.

9. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1880, 1894 (2013).

Part I briefly explores the evolution of health technology, including the shift from fiduciary and context-rich relationships to more attenuated human-computer interfaces. Part II discusses a brief history of consent in health care, including social developments that led to privacy concerns and a desire to address them. In Part III, I apply Helen Nissenbaum's concept of contextual inquiry to examine the failure of consent as choice resulting from five distinct problems, the "consent myth." Part IV responds to these problems by proposing four principles to improve choice for more effective consumer engagement advancing individual autonomy.[10]

I. HEALTH TECHNOLOGIES FRUSTRATE TRADITIONAL PRIVACY LAW REGIMES

Modern health technologies include everything from websites providing disease information to mobile health apps and home health robotics. These technologies have intensified privacy debates, especially when technology incorporating Internet connectivity or large data collection creates new potential risks to the individual, such as data misuse or loss through cyberattacks.[11]

The Internet of Health Things (IoHT) is a technology that connects physical devices, such as medical devices, with the Internet. The IoHT, which include the Internet of Medical Things (IoMT), is a variation of the well-known Internet of Things (IoT), or the conversion of self-contained analog consumer devices to increasingly Internet-tethered consumer devices.[12] IoHT devices span the marketplace of health-related devices: connected medical devices, consumer self-care, and health improvement technologies.[13] IoHT devices are produced by highly regulated market sectors, such as health care and medical device manufacturing, as well as the comparatively less-regulated consumer product manufacturing.[14] IoHT devices include everything from connected pacemakers to mobile device-

10. The consent myth and resulting principles to address it may also apply to additional consumer contexts. Here, we have narrowed the field for purposes of clearly articulating how contextual differences may create problems for new technologies.

11. *See* Tschider, *supra* note 3, at 187.

12. Nicolas P. Terry, *Will the Internet of Things Transform Healthcare?*, 19 VAND. J. ENT. & TECH. L. 327, 329 (2016); *IoMT (Internet of Medical Things) or healthcare IoT*, TECHTARGET, https://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things [https://perma.cc/T73V-S9FF] (last updated Aug. 2015) [*hereinafter* Terry, *IoT*]; Bernard Marr, *Why the Internet of Medical Things (IoMT) Will Start to Transform Healthcare in 2018*, FORBES (Jan. 25, 2018, 1:41 AM), https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-totransform-healthcare-in-2018/#733399274a3c [https://perma.cc/R4PP-YMHU]; S. M. Riazul Islam, Daehan Kwak, MD. Humaun Kabir, Mahmud Hossain & Kyung-Sup Kwak, *The Internet of Things for Health Care: A Comprehensive Survey*, 3 IEEE ACCESS 678 (2015) [*hereinafter* Islam et al.].

13. *See* Terry, *IoT*, *supra* note 12.

14. *See infra* Part II and accompanying notes.

connected insulin pumps, Internet-connected X-Ray machines, and fitness trackers.

A. Privacy and IoHT

IoHT devices are unique in that these devices directly collect personal data through automated and pervasive interaction, which may or may not implicate device security and safety.[15] IoHT, then, can be understood as a type of continuous surveillance, wherein data are collected by private organizations for any number of purposes. These purposes likely include consumer-expected data uses, such as product registration, basic device functionality, or product improvement activities, but may also include more attenuated purposes designed to benefit the consumer or the manufacturer. IoHT manufacturers may anticipate financial benefits not only from selling IoHT devices but also from data collection efforts.[16]

IoHT devices may collect a wide variety of data as part of functionality and the human-computer interactive model. The data may differ in data sensitivity, for example from an individual heart rate or evidence of a serious disease to what a person might have eaten for breakfast. These data, for most IoHT implementations, will be combined with other data collected, bought, or exchanged, sometimes about the same users.[17] These other data feed big data implementations, which power the "smart" aspect of IoHT offering advanced analytics, improved algorithm performance, or even feeding machine learning utilities.[18] Data collected as part of big data sets both have utility for an effective IoHT implementation and simultaneously may provide personally identifiable health data or proxies for these data.[19]

---

15. *See* Terry, *IoT*, *supra* note 12, at 342–43.

16. Krista Kennedy observes that "one must learn to work closely with a machine that is inserted into a bodily orifice and whose consistent use affects cognitive processing and neural pathway development." Krista Kennedy, *Designing for Human-Machine Collaboration: Smart Hearing Aids as Wearable Technologies*, 5 COMM. DESIGN Q. 40, 41 (2017) (describing how the hearing aid, an IoHT device, requires human interaction to function properly to the advantage of the human).

17. Big data are defined by the four "Vs": volume, variety, velocity, and veracity. Data was "getting big" before the advent of the IoT, but the IoT have injected substantial volume and variety, with increased velocity and veracity. These data sets will likely include data of IoT provenance, with other data, as well. *See* Charles McLellan, *The Internet of Things and Big Data: Unlocking the Power*, ZDNET (Mar. 2, 2015, 9:39 AM), https://www.zdnet.com/article/the-internet-ofthings-and-big-data-unlocking-the-power/ [https://perma.cc/5NT7-E35D].

18. Improved functionality results from integration of IoT devices with large data sets powering machine learning utilities, which use big data sets to develop powerful algorithms. *See*, *e.g.*, Islam et al., *supra* note 12, at 683 (describing the variety of data layers and sources in IoHT technical implementations); Prashant Natarajan Iyer, *A Tale of 2 T's: When Analytics and Artificial Intelligence Go Bad*, HEALTHCARE IT TODAY (July 13, 2016), https://www.emrandhipaa.com/author/prashant/ [https://perma.cc/4UD6-P24Y].

19. There are tremendous benefits to data collection and use, especially for patient care and research purposes. *See* W. Nicholson Price II, *Black-box Medicine,* 28 HARV. J.L. & TECHN. 419, 435

It is often unclear, at the time of device purchase or prescription, which data may exist in the data set overall, their provenance, and their overall degree of identifiability within the broader data set. For these reasons, IoHT introduces a special type of privacy risk for consumers and patients when it is implemented using cutting-edge technologies like big data sets and machine learning utilities.[20] However, the degree of legal protection afforded patients or consumers often differs based on how the device is procured, rather than what the device can do.[21]

One particularly interesting example of legal protection inconsistency involves hearing aids. Nearly 37.5 million adults have a hearing impairment, and only a fraction of those adults use hearing aids (from 16–30%, depending on age).[22] To solve hearing aid access issues, Congress passed over-the-counter hearing aid legislation in 2017, which permits hearing aid companies to sell hearing aids directly to consumers.[23]

Although the availability of hearing aids to a broader population might satisfy an important public good, smart hearing aids also illustrate a compelling example of inconsistent regulation for IoHT devices. Modern hearing aids employ cutting edge technologies, including geolocation and predefined settings associated with automatically defined physical spaces, to improve aid performance.[24] These aids now connect to mobile devices and can be controlled through a mobile application.[25] Hearing aids prescribed through a health care provider that processes payment, such as insurance reimbursement, will likely be regulated by the Health Insurance Portability and Accountability Act (HIPAA).[26] HIPAA mandates specific notice and authorization requirements, as well as additional privacy and security rule standards, depending on the nature of data collection and use.[27]

Hearing aids available over-the-counter, regardless of whether they are identical to prescribed devices, will likely only need to meet a

(2015); Charlotte A. Tschider, *Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DEN. L. REV. 87, 99 (2018).

20. *Tschider*, *supra* note 19, at 104.

21. *See* Terry I, *supra* note 12, at 339 n.82; Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385, 386 (2012).

22. *Quick Statistics about Hearing*, NAT'L INST. ON DEAFNESS & OTHER COMM. DISORDERS, https://www.nidcd.nih.gov/health/statistics/quickstatistics-hearing [https://perma.cc/468V-B5ND] (last updated Dec. 15, 2016).

23. *US Senate Passes OTC Hearing Aid Act as Part of FDA Reauthorization Act of* 2017, HEARING REV. (Aug. 4, 2017), http://www.hearingreview.com/2017/08/us-senatepasses-otc-hearing-aid-act-part-fda-reauthorization-act-2017-ada-announces/ [https://perma.cc/Y4PT-QQQA].

24. Sarah Bricker, *Tech Tip: How to Manage Your Hearing Aid Memories*, STARKEY HEARING TECHNS. (Dec. 13, 2016), https://www.starkey.com/blog/2016/12/trulink-hearing-aid-memories [https://perma.cc/4KPW-5NXE].

25. *Id.*

26. *See infra* Part II and accompanying notes.

27. *See infra* Part II and accompanying notes.

comparatively lower threshold of not engaging in "unfair or deceptive trade practices."[28] Although organizations selling these hearing aids must not engage in unfair or deceptive trade practices, the Federal Trade Commission (FTC) does not otherwise mandate any specific privacy model: the model is responsive rather than preventative.[29] Between the HIPAA and FTC models, the HIPAA model is more restrictive but narrowly applies to predefined organizations that fit specific HIPAA definitions. Therefore, differential obligations for otherwise identical devices collecting and using identical data illustrate a fundamental problem in how the United States protects consumer and patient privacy interests in relation to IoHT. Privacy regulation for the same or similar IoHT devices might result in vastly different compliance, none of which may effectively support consumer choice. And choice becomes more important as privacy risks increase. For example, location data collected could present greater privacy risks when those data are shared with or sold to third parties for commercial or aggregation purposes. Geological data may establish patterns of behavior, movement, or frequently visited locations.

B. Human-Computer Interaction

Almost all IoHT, like smart hearing aids, automate features and functions that historically required a human actor for some intervention, such as a medical doctor interpreting data. The effect of automation, a precursor to more advanced forms of AI,[30] has been an increasing opacity in relation to data collection and use due to the removal of human actors and their attendant relationships of trust.[31] While traditional human-to-human relationships involve some communicative mechanisms and opportunities

28. *See infra* Part II and accompanying notes. A finding of unfair trade practices or deceptive trade practices is a responsive, *ex post* determination, rather than providing any *ex ante* set of requirements.

29. *See infra* Part II and accompanying notes. The FTC has not passed any specific rules at the same level of stringency as mandated under HIPAA.

30. Kamila Hankiewicz, *What Is the Real Difference Between Automation and AI?*, BECOMING HUMAN (Aug. 9, 2018), https://becominghuman.ai/what-is-the-realdifference-between-automation-and-ai-366513e0c910 [https://perma.cc/5GG7-4FF7].

31. *Id.*; *see infra* Part III and accompanying notes. The concept of trust has historically been a product of human-to-human relationships. By replacing or distancing human-to-human relationships, artificially intelligent and connected machines complicate traditional trust relationships, especially of a fiduciary nature (e.g., the doctor-patient relationship). *See* Robin C. Feldman, *Artificial Intelligence: The Importance of Trust & Distrust*, 21 GREEN BAG 2D 201, 206–07 (2018). Feldman describes the changing dynamics of trust in AI-enabled contexts, including both over-confidence and lack of trust in human-computer interactions. "[T[rust and distrust can wrap back around each other and collide to provide the maximum risk for chaos and societal disruption." *Id.* at 209.

for inquiry and response, the human-to-computer interface offers comparatively fewer opportunities.[32]

When human-to-computer interfaces supplant human-to-human relationships, traditional privacy contexts do not necessarily transfer to these new interfaces, especially the privacy notion of "choice." As a result, consent may not effectively reinforce important patient and consumer privacy interests or enhance trust relationships in new IoHT contexts where downstream data uses and associated privacy risks cannot be effectively described in the privacy notice.[33]

II. CONSENT AND THE LAW

Consent as a legal mechanism in privacy law originally extended from the commercialization of historically personal relationships in 17th and 18th Century Europe, where commercialization divorced individuals from local economies.[34] However, until the early 1900s, doctors and other medical practitioners within a small community still provided healthcare.[35] Provisioning healthcare was often framed by a relationship of personal trust between a medical practitioner and an individual patient, a fiduciary relationship hallmarked by a vulnerability of one individual within the relationship due to information asymmetries.[36]

Consent, "an act of reason accompanied with deliberation,"[37] initially developed as a means for negotiating disclosures between the private self

32. *See* Kennedy, *supra* note 16. Kennedy notes the existence of human-computer collaboration as a phenomenon resulting from pervasive technology and human interactions, where a human must rely on technology for functionality. It is this Author's view that this relationship does not provide the same opportunities for communication about individual privacy.

33. It should be noted that this Author also questions whether consent is the appropriate mechanism for traditional relationships involving the transfer of personal information. However, the use of consent in human-to-computer contexts is much more problematic, as explained through the remainder of this Article.

34. After the 17th Century, the public and private spheres began to connect in important ways, especially related to commerce and information dissemination. However, local communities became substantially more reliant on regional and national markets. These two simultaneous movements transformed how individuals participated in both the market and their personal lives. JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY LAW, ETHICS, AND THE RISE OF TECHNOLOGY 9 (1997); *see also*, JÜRGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE 3 (Thomas Burger trans., 1991).

35. The Gale Group, Inc., *The 1900s Medicine and Health: Overview*, ENCYCLOPEDIA.COM (2003), https://www.encyclopedia.com/socialsciences/culture-magazines/1900s-medicine-and-healthoverview [https://perma.cc/7KEG-6CEU]. By way of example, in 1900, most doctors performed surgeries at their patients' homes. *Id.*

36. Fiduciary relationships usually involve sensitive or high-stakes circumstances, where forming the relationship (and receiving services) is a public good (such as improving health) or where the reliant and more vulnerable party could lose something substantial (e.g., freedom, money, or employment). *See* Daniel J. Solove, *A Taxonomy of Privacy,* 154 U. PENN. L. REV. 477, 522 (2006).

37. BLACK'S LAW DICTIONARY ONLINE, *Consent*, https://thelawdictionary.org/consent/ [https://perma.cc/PA7Q-D5FQ] (last visited Mar. 4, 2019).

and the public marketplace, ultimately becoming a proxy for choice that accompanied individual medical practitioner-patient relationships.[38]

A. Consent under the Health Insurance Portability and Accountability Act

Technical advancements in computerized medical record-keeping and a desire for administrative efficiencies prompted examination of privacy concerns outside common law and statutory solutions in healthcare.[39] In 1996, HIPAA became the first federal privacy law passed in the health care sector, although details of the Privacy Rule followed in 2003.[40]

The HIPAA Privacy Rule, as implemented, requires Covered Entities (CEs) to display (or outsource display of) an annual notice of privacy practices for uses related to treatment, payment, and health care operations.[41] Although consent is not required, treatment providers (health care providers) must make a "good faith effort" to obtain the individual's written acknowledgement of notice receipt.[42]

Implicitly, HHS's HIPAA notice provides better information when individuals have contextual cues regarding their privacy or can ask questions of their medical practitioner.[43] For example, it is not unexpected

38. Within small communities, unauthorized disclosures of health information eventually became a concern when sensitive information was shared with others in the community. Consent, therefore, became an inexpensive way to safeguard against legal claims of confidentiality breaches. *See* Daniel J. Solove, *A Brief History of Information Privacy Law, in* PROSKAUER ON PRIVACY, PLI 5, 17 (2006) (quoting *Simonsen v. Swensen*, 177 N.W. 831 (Neb. 1920), in which the court identified a 'wrong' and recognition of damages for loss of confidentiality), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2076&context=faculty_publications [https://perma.cc/LA5A-BMHT].

39. Donna Bowers, *The Health Insurance Portability and Accountability Act: Is It Really All That Bad?* 14 BAYLOR UNIV. MED. CTR. PROC. 347 (2001) It should be noted that HIPAA was originally created for insurance portability purposes, which explains its narrow application to specific covered entities.

40. 45 C.F.R. §§ 160, 164 (2018); HIPPA, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033-34 (1996); *see* Gina Marie Stevens, *CRS Report: A Brief Summary of the HIPAA Medical Privacy Rule*, CONGRESSIONAL RESEARCH SERVICE (Apr. 30, 2003), https://digital.library.unt.edu/ark:/67531/metacrs5165/m1/1/high_res_d/RS20934_2003Apr30.pdf. *See also* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 714–15 (2007) (discussing the limited efficacy of HIPAA privacy with respect to electronic health records).

41. 45 C.F.R. § 164.520 (2018). The Privacy Rule has not been updated since its final passage in August 2002. Although timing for providing the Notice of Privacy Practices differs depending on the type of CE, ideally the notice is provided prior to an individual providing Protected Health Information (PHI) to the CE or its Business Associates (BAs).

42. *Id.*

43. Implied consent as is implemented for primary data uses under HIPAA (consent by virtue of opportunity to read and desire to receive service) relies on clear contextual information. Authorization, in contrast, communicates uses outside typical context, which requires additional confirmation of understanding and explicit consent to specifically defined uses. *What is the Difference between "Consent" and "Authorization" under the HIPAA Privacy Rule?*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/forprofessionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html [https://perma.cc/VKN8-8SPQ].

that an individual's health data will be used in connection with providing health treatment, or that it might be relevant for receiving health insurance reimbursement. When personal information collection, use, or transfer is reasonably expected because a contextual framework exists, notice improves individual awareness by building on existing expectations. Because data use and transfer are tightly linked to operational processes, high-context data processing is sometimes called *primary use*.[44]

HIPAA requires additional authorization outside operational activities, and when using and disclosing PHI to adhere to the "minimum necessary" for specifically communicated uses.[45] HIPAA authorization operates like explicit consent, or consent that requires specific and clear manifestation of an individual's agreement.[46] Under HIPAA, authorization is reserved for operational uses beyond those directly communicated and connected to provisioning health care treatment, facilitating application of insurance reimbursement, and billing processing.[47] Authorization includes disclosure to another facility, physician, clinic partners, involvement of third parties, or additional data uses (e.g., research, product improvement, data sharing).[48]

To fully complete the authorization process, a CE must gather an individual's explicit consent prior to PHI collection or disclosure using a detailed authorization document.[49] For example, authorization procedures will be used when medical records are transferred to a new facility, such as when the patient has requested this transfer or has been referred by a general practice physician to a specialty doctor.[50] In that circumstance, not only is a patient reading an authorization form that communicates the reason for data transfer, patients often fill out the authorization form with a doctor or nurse present and available to explain the purpose for authorization. CEs likely facilitate HIPAA authorization when the individual has some context for understanding the data transfer, such as when explaining the need for another medical procedure or future service.

Authorizations may be used for a wide variety of less common purposes, such as disclosing records to another family member, when third parties

---

44. Charles Safran, Meryl Bloomrosen, W. Edward Hammond, Steven Labkoff, Suzanne Markel-Fox, Paul C. Tang & Don E. Detmar, *Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper*, 14 J. AM. MED. INFORM. ASSOC. 1, 4 (2007).

45. 45 C.F.R. § 164.506.

46. *Id.* Authorization must be expressed and written in nature.

47. *What is the Difference between "Consent" and "Authorization" under the HIPAA Privacy Rule?*, *supra* note 43.

48. *Id.*

49. *Id*. Authorization documents must include the following information: description of PHI to be used and disclosed, expiration date, purpose for which the information is used or disclosed. Provisioning health services cannot be conditioned on the individual executing an authorization.

50. *Id.* (describing authorization as the means to use PHI for purposes other than operations).

wish to use such information for product development purposes, or when a clinician wishes to use previously collected data for research purposes. Commonly, authorizations are used for third party data transfer.[51] Use requiring authorization is commonly called *secondary use*, because the desired use is not implicit in the purpose under which it was originally collected.[52]

A lack of clear direction has created confusion and potential efficiency issues for large information databases, including those that may provide the infrastructure for IoHT functionality.[53] Further, healthcare consent and authorization disproportionately affects organizations with many discrete, non-operational uses.[54] HIPAA requires authorization for each specific use, which means that organizations storing data in a large database and running clinical trials may have to execute, store, and update (as necessary) two or more authorizations for each participant in addition to informed consent required for human research.[55]

Although this health privacy framework might appear fairly comprehensive, the scope of ethical oversight and laws is actually quite narrow. Many organizations, especially those creating new technologies and those that do not receive insurance payment for services, usually will not be regulated by HIPAA as a Covered Entity or a Covered Entity's Business Associate or be bound under traditional confidentiality obligations, as might be obligated under a fiduciary relationship. Organizations manufacturing, distributing, or offering services for IoHT devices, medical applications (such as mobile health apps), telehealth, or out-of-pocket health care, may not qualify as either a Covered Entity or a Business Associate.[56] Given

51. Third party data transfer is presupposed by HIPAA's interoperability and portability goals: an individual should benefit from integration with other facilities and be able to exercise preference in care. However, many of these transfers may actually be permitted by HIPAA without explicit consent. *See Understanding Some of HIPAA's Permitted Uses and Disclosures*, U.S. DEP'T HEALTH & HUM. SERVS. (Feb. 12, 2016), https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/permitted-uses/index.html [https://perma.cc/HN2E-W7W9].

52. SHARON HOFFMAN, ELECTRONIC HEALTH RECORDS AND MEDICAL BIG DATA 20 (2016).

53. 45 C.F.R. §§ 46.116, 46.117; U.S. DEP'T HEALTH & HUM. SERVS., NAT'L INSTS. HEALTH, PUB. NO. 04-5489, RESEARCH REPOSITORIES, DATABASES, AND THE HIPAA PRIVACY RULE (Jan. 2004), https://privacyruleandresearch.nih.gov/research_repositories.asp [https://perma.cc/3M3C-ZTKN]. Certainly, arguments could easily be made in favor of strict authorization requirements. Authorization serves an important purpose: to specifically notify an individual of additional uses and secure explicit consent for purposes of patient awareness, to diminish potentially excessive or abusive practices, and to reduce potential for misuse or fraud. However, the potential benefit of future data use across organizations in furtherance of scientific or research goals certainly is very persuasive.

54. *Id.*

55. *Id.*

56. Covered Entities are defined as health care providers (when transmitting electronic PHI for insurance-qualifying purposes), a health plan (insurers, company health plans, government programs, and Health Maintenance Organizations), or a health care clearinghouse that process nonstandard health information into as standard format. 45 C.F.R. § 160.103. BAs are persons or entities that perform functions or activities on behalf of a CE for HIPAA-applicable purposes. BAs can perform legal,

HIPAA's narrow application, it is likely emerging health technology might only be regulated by the general oversight of the Federal Trade Commission (FTC).

B. Consent under the FTC's Fair Information Practices (FIPs)

In the early 2000s, the FTC expanded on Fair Information Practices originally identified by the U.S. Department of Health, Education and Welfare (HEW) (1973), subsequently defining these practices as "Notice, Choice, Access, and Security," with FTC enforcement.[57] Notably, HEW's choice principle delineated between internal, or primary, and external, or secondary, uses.[58] After HEW's initial articulation of the Fair Information Practices, the FTC has increasingly used the term *consent* interchangeably with *choice*.[59] In contemporary FTC communications to organizations doing business in the United States, these discrete concepts appear to have merged or at least have been linked, prompting the facial misunderstanding that consent *is* choice.[60] Consent, therefore, has become a legally defensible piece of evidence for most information handling practices:[61] if an organization provides a privacy notice and solicits explicit consent, the organization has met its obligation, regardless of the notice's contents, so

---

actuarial, consulting, aggregation, management, administrative, accreditation, or financial services. *See Business Associates*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/businessassociates/index.html [https://perma.cc/3V7W-YJAW]. *See Adopted Standards and Operating Rules*, CTRS FOR MEDICARE AND MEDICAID SERVS. (Oct. 23, 2017), https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAAACA/AdoptedStandardsandOperatingRules.html [https://perma.cc/7EBU-F33Z].

57. *See* INTERNAL REVENUE SERVICE, STATISTICAL USES OF ADMINISTRATIVE RECORDS: RECENT RESEARCH AND PRESENT PROSPECTS 472 (Jan. 1, 1984). FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [https://perma.cc/8EMY-MT8A].

58. *Id.* By any indication, the FTC seems to observe a difference between expected and unexpected uses, wherein initial personal information collection and use ties directly to provisioning services or providing products. However, other uses may be less expected from the point of initial relationship formation, making actual "choice" a more attenuated concept.

59. *See*, *e.g.*, FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 8 (June 1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf, (describing 'choice' by describing consent options in Web environments and other mechanisms for parental consent) [*hereinafter* FTC 1998]; FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2016 2 (2016), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf [https://perma.cc/MV87-HZLE] (referencing choice *mechanisms*). It is important to acknowledge that choice, as a concept, reflects a mental process and subsequent action, including inaction. Consent, however, is often considered a procedural mechanism. Trading consent for choice substitutes both the mental process and action with only a procedural mechanism.

60. *See* FTC 1998, *supra* note 59.

61. Solove, *supra* note 9.

long as the contents are not misleading or incorrect (deceptive).[62] As the FTC has noted: "If a consumer is provided with clear and conspicuous notice prior to the collection of information, there is no basis for concluding that a consumer cannot generally make an informed choice."[63]

The United States has created, at best, a layered and accretive regulatory privacy regime; at worst, an inconsistent and ineffective framework. Although HIPAA and the FTC's Fair Information Practices each introduce slightly different models for facilitating consumer choice, none of these address the core issue: using consent as a proxy for individual choice.[64]

III. THE CONSENT MYTH

Although consent has been positioned as a proxy for choice, privacy law's goals should advance individual autonomy, rather than simply giving the appearance of legitimacy. Helen Nissenbaum's reflections on contextual inquiry provide a philosophical-legal lens through which the use of consent is legitimate or problematic in relation to its context. The "consent myth" aggregates privacy's failings with respect to consent for purposes of confronting these issues and finding comparatively better models to advance individual choice.

A. Evaluating Autonomy, Context, and Choice

Consent, as a concept, emerged from the common law as something similar to, yet apart from, legal concepts of agreement within contract, and Congress and administrative agencies accepted and adopted this model. Black's Law Dictionary defines "consent" as something more than simply

62. Although Section 5 permits the FTC to enforce against unfair or deceptive trade practices, characteristically, the FTC has primarily focused on deceptive practices, likely because these practices are easier to prove.

63. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS 15, E-5 (Dec. 2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf [https://perma.cc/2482-VQ4K] [*hereinafter* FTC 2010].

64. It should be noted that the General Data Protection Regulation, 2016/679 updating the European Union's (EU) oft-copied Data Protection Directive, 95/46/EC, requires explicit consent for sensitive data collection and use, while permitting individual countries derogation. This derogation permits individual countries to completely bar sensitive data collection. Further, consent, specified in Article 7, must pertain to discrete data uses. However, consent is not the only valid lawful basis for data processing. In addition to legal obligations, contract, vital interests, and public activities, the EU also permits data be processed for certain "legitimate interests" in the GDPR's Recital 47, which incorporates a balancing test. This balancing test illustrates a recognition by the EU that in some cases, an organization's interests may outweigh an individual to process data without consent or another valid lawful basis. Although this article focuses on the United States' approach to consent, the concept of legitimate interest may offer an alternative to consent for some data uses, especially for large database collection.

a formulation of agreement. Consent is something personal that requires individual engagement: "a concurrence of wills, an act of reason accompanied with deliberation."[65]

Helen Nissenbaum has described information distribution norms including relational concepts of free choice, discretion, and confidentiality, expected in fiduciary relationships, as well as need, entitlement, and obligation, concepts typical of contractual relationships.[66] Autonomy informs choices made when "guided by principles . . . adopted as result of critical reflection."[67] Presumptively, an individual can only legitimately exert choice when an individual can exercise autonomy,[68] and autonomous life involves choices after "full deliberative rationality . . . with full awareness of facts and after careful consideration of the consequences."[69] Privacy can be defined as a form of autonomy, self-determination regarding one's personal information through choice about its collection and use.[70]

Privacy has a broader social value and context, in that it fulfills important social and personal functions, such as reinforcing a healthcare relationship where information exchange is crucial to effective treatment.[71] Nissenbaum sees benefit in both recognizing these important functions and the free-flow of information, injecting the concept of contextual integrity.[72] Contextual integrity examines norms and expectations while considering informational relationships to context, individual roles, role relationships, rules of flow, and impact on underlying values.[73]

Although traditional healthcare environments may provide more effective contextual cues and real assistance related to privacy concerns,

65. BLACK'S LAW DICTIONARY ONLINE, *supra* note 37.

66. Helen Nissenbaum, *Privacy as Contextual Inquiry*, 79 WASH. L. REV. 119, 124 (2004).

67. *Id.* at 130 (reflecting on theories advanced by Gerald Dworkin, Ruth Gavison, Jeffrey Reiman, and Julie Cohen).

68. *Id.*

69. JOHN RAWLS, A THEORY OF JUSTICE 408 (1971). Certainly "thicker" autonomy proponents might argue for a greater recognition of *caveat emptor*, especially as this applies in circumstances with multiple choices. However, for privacy, exogeneity issues combined with substantial bargaining power disparities (especially for markets with few alternatives) reduce the ability for an individual to completely negotiate to their own benefit. Health contexts present inherently unequal bargaining models, which is why fiduciary duties often co-exist in these contexts.

70. HELEN NISSENBAUM, PRIVACY IN CONTEXT 81–82 (2010).

71. *Id.* at 132 (quoting Priscilla Regan). Janlori Goldman has also described the essential function of privacy for medical purposes: without "robust protections," individuals will not seek medical care or advance research interest. *See also*, JERRY BERMAN & JANLORI GOLDMAN, BENTON FOUNDATION PROJECT ON COMMUNICATIONS & INFORMATION POLICY OPTIONS, A FEDERAL RIGHT OF INFORMATION PRIVACY: THE NEED FOR *REFORM* 32 (1989), https://files.eric.ed.gov/fulltext/ED324011. pdf [https://perma.cc/2NRY-SBTW] (identifying the need for a federal privacy law, including more restrictions for sensitive data use and data uses above what is disclosed). Privacy reinforces the quality of fiduciary relationships by enhancing trust, and fiduciary relationships usually involve some commitment of privacy, to the benefit of the dependent party. NISSENBAUM, *supra* note 70, at 132.

72. NISSENBAUM, *supra* note 70, at 136.

73. *Id.*

upon contextual inquiry, a primary issue emerges that, at its root, undermines consumer choice. First, individuals alone may not be able to influence outcomes in their interest because privacy bargaining occurs through relationships with substantial power differentials (implicit in healthcare relationships) and within an inherently adhesive bargaining scheme. When individuals have few opportunities to freely bargain and cannot make an effectively informed choice due to other information asymmetries, individuals cannot ultimately fulfill their own privacy interests: they have no actual "choice."

In broad strokes, privacy law has dual aims: 1) to advise individuals of planned activities involving their data, so that individuals can make choices about these practices, and 2) to not impose arduous requirements on commercial activities employing these practices. The current consent mechanism alerts an individual to activities involving personal data without actually advising individuals of the risk.

B. Consent's Problems

Although personal information collected under a highly regulated health care privacy regime does enjoy better comprehensive privacy practices, the superimposition of consent for choice has caused a number of problems for individual autonomy.

The Consent Myth is a set of five problems that build on each other: the voluntariness problem, the structural problem, the cognition problem, the exogeneity problem, and the temporal problem. Each problem evidences a way in which consent has failed to effectively support autonomous choice, to varying degrees, depending on the context in which an individual or product exists.

1. Consent Myth 1: Individuals Have Meaningful Choice When Privacy Notices are Used (Voluntariness Problem)[74]

Most privacy policies (including a Notice of Privacy Practices) would be defined as contracts of adhesion. Contracts of adhesion are called adhesive contracts because they involve one-sided practices: essentially, a "take it or leave it" model and evidence unequal bargaining power.[75] This can be problematic especially in the health care industry, whether highly regulated

74. When individuals cannot voluntarily consent, they cannot be said to have "informed consent." Further, many privacy policies and terms of service are similar between potential competitors (or at least appear to be similar to a consumer), so the concept of market competition often does not apply.

75. Nora K. Duncan, Adhesion Contracts: A Twentieth Century Problem for a Nineteenth Century Code, 34 LA. L. REV. 1081 (1974).

or less regulated, because typically: 1) individuals often require or depend on services or products to survive or to improve their lives, 2) individuals inherently trust organizations operating in the health care sector because of existing medical confidentiality relationships, and 3) alternative options may not exist in the marketplace. Contract law does recognize a legal limit on contracts of adhesion: unconscionability.[76]

Contracts of adhesion are not inherently coercive. They are, however, common in privacy policies: coercive privacy practices often include "bundling" of terms together in one agreement.[77] Bundling makes reading privacy policies longer and subsequently more difficult to read, which in turn makes these likely to be ignored.[78] In addition to these coercive issues, trust also plays a role in interpreting privacy policies and their relative fairness, for consent purposes. As described by many scholars, focusing on the concept of trust in relationships can offer an opportunity for understanding what duties are owed to each party.[79] Sometimes, trust is misplaced, not because one party breached any confidential relationship, but because an organization benefitted from some transference of trust.[80] Organizations under the auspices of "health technology" often benefit from this transference, and because often organizations provide products or

76. Arthur A. Leff, *Unconscionability and the Code: The Emperor's New Clause,* 115 U. PA. L. REV. 485, 467 (1967)

77. *See,* Twila Brase, *HIPAA's Unhealthy Privacy Deception*, CNS NEWS (Dec. 15, 2014), https://www.cnsnews.com/commentary/twila-brase/hipaa-s-unhealthy-privacy-deception [https://perma.cc/FYG8-3U9M]; Bojana Kostić & Emmanuel Vargas Penagos, *The Freely Given Consent and the "Bundling" Provision under GDPR*, COMPUTERRECHT 2017/153 (Apr. 2017), https://www.ivir.nl/publicaties/download/Computerrecht_2017_4.pdf [https://perma.cc/6X5P-K3UR].

78. It could potentially be argued, although not explored at length in this article, that bundled privacy policies *per se* meet procedural unconscionability requirements due to their coercive status, should the terms themselves be excessively one-sided. The European Union has explicitly barred these types of notices precisely for this reason.

79. *See infra* Part II.A and accompanying notes; Helen Nissenbaum, *Respecting Context to Protect Privacy: Why Meaning Matters*, SCI ENG. ETHICS (2015), DOI: 10.1007/s11948-015-9674-9 [*hereinafter* Nissenbaum 1]. As the Obama Administration noted in 2012, "Respect for Context" means that organizations will collect data in a manner consistent with the context in which individuals provide such data. In practice, typical health care contexts likely provide ample contextual cues to determine whether data use or transfer is reasonable or not, especially when less straightforward uses require a specialized form and explicit consent. However, context also includes relationships between individual and the health data receiver. *Id.* This relationship creates either an express or inherent confidentiality expectation, which likely increases the degree of trust between the parties. When health data is used and shared within this context over time, trust usually accompanies the exchange. *See, e.g.*, Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 457 (2016) [*hereinafter* Richards & Hartzog] (describing fiduciary relationships as a foundational concept for trust by 'reorient[ing] privacy and crystalliz[ing] the concept of trust in information relationships).

80. Katherine Stewart, *Transference as a Means of Building Trust in World Wide Web Sites*, ICIS 1999 PROCEEDINGS, PAPER 47, 460 (1999). Trust is transferred when one organization transfers, refers, or creates a relationship with the other. Therefore, products or services recommended (even when not insurance-eligible or HIPAA-regulated) by a physician likely will be perceived as higher trust products or services. Increasingly, physicians have recommended any number of commercial products or services, from connected scales to Fitbits.

services individuals need, these individuals cannot afford not to trust them.[81] When health organizations provide services, there are not always alternatives to the type of care or technology an individual wishes to purchase. Contracts of adhesion, as a legal model, work somewhat effectively when many options exist, such as eight different coffee maker models, not when an individual needs an insulin pump.[82]

2. Consent Myth 2: Consumers Would Read Privacy Policies If They Cared Enough (Structural Problem)[83]

The connected consumer is bombarded with privacy policies so frequently today, a term has emerged for it: *privacy policy fatigue*. Several studies, from 2005 to today, illustrate that consumers often do not read privacy policies. In 2005, a few years after the Privacy Rule was implemented, 59% of patients recall receiving a privacy policy and 27% believed they had more rights than they did.[84] In 2006, only 20% of people read privacy policies "most of the time."[85] Is it legally reasonable, then, to assume consent in these cases is legally binding? In 2014, a Pew Internet Study demonstrated that half of Americans could not explain the term "privacy policy."[86]

Fewer people read terms of use agreements fully, which often contain privacy language. According to one 2011 study, only 1% of consumers read the terms.[87] Some studies have resulted in comical results. In one study, 22,000 people agreed to clean toilets and other undesirable tasks for free Wi-Fi, with only 1 in 22,000 objecting to the terms of use.[88] Jonathan Obar

---

81. *Id.*

82. This makes intuitive sense: if contracts of adhesion were deemed legal from an efficiency in economics perspective (i.e., it is too time-consuming to negotiate every consumer agreement, which reduces profits), likely it presumed that *caveat emptor* would guide these decisions, and that alternatives existed. In the healthcare space, especially healthcare technology, often alternatives do not exist.

83. *See* Solove, *supra* note 9, at 1888.

84. INSTITUTE OF MEDICINE (US) COMMITTEE ON HEALTH RESEARCH AND THE PRIVACY OF HEALTH INFORMATION: THE HIPAA PRIVACY RULE (2009), https://www.ncbi.nlm.nih.gov/books/NBK9579/ [https://perma.cc/BUA4-GAGU].

85. *See* Solove, *supra* note 9, at 1884 n.14 (quoting Helen Nissenbaum's articulation of a TRUSTe & TNS study).

86. *See* Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR (Dec. 4, 2014), http://www.pewresearch.org/facttank/2014/12/04/half-of-americans-dont-know-what-aprivacy-policy-is/ [https://perma.cc/8KJ7-FB5R].

87. Solove, *supra* note 9, at 1884 n.15 (citing Omri Ben-Shahar & Carl E. Schneider's discussion of a study in Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 665–78 (2011)).

88. Christopher Burgess, *Wait, You Didn't Want to Clean the Toilets? Should Have Read the Terms!*, NAKED SECURITY (July 17, 2017), https://nakedsecurity.sophos.com/2017/07/17/wait-you-didnt-want-to-clean-the-toilets-should-have-read-the-terms/ [https://perma.cc/KK36-ADUW]; Jonathan A. Obar & Anne Oeldorf-Hirsch [Obar & Oeldorf-Hirsch], *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, INFO COMM. & SOC'Y 1,

and Anne Oeldorf-Hirsch tackled this issue, finding that 98% of individuals will miss these clauses.[89] It is clear that consumers have been conditioned not to read things that look like legal documents, regardless of whether privacy language is included. There is a structural problem associated with policy fatigue: even "well-informed and rational" individuals cannot appropriately self-manage.[90]

Consumers in many cases cannot afford to spend the time. One study approximated the time to read every privacy policy at seventy-six work days a year.[91] Despite available time, cognitive limitations further restrict the degree individuals can take in all appropriate information across all privacy policies a consumer might encounter.[92]

In these cases, although logic might tell us a consumer *would* allocate time to read these privacy policies due to the perceived inherent risk; instead, it is more likely that consumers would have a false sense of security and assume someone else will ensure these notices are "fair." Individuals may even assume the presence of a notice at all means the organization has strong privacy practices, which may not be accurate.

3. Consent Myth 3: Plain Language Makes Privacy Policies Understandable (Cognition Problem)[93]

Although the plain language movement has improved the readability of privacy policy language,[94] individuals still have a difficult time understanding what the language really means, to say nothing of vulnerable populations, differential reading levels, disabilities that make the traditional privacy policy less accessible to certain populations, and individuals where English is a Second Language (ESL).[95] For example, if privacy policies are truncated and specific, often they leave out important details that make information "real" for the consumer; when privacy policies provide more

16 (2016), https://doi.org/10.1080/1369118X.2018.1486870. Additionally, 93% of participants agreed to the Terms of Service, 97% of participants agreed to the privacy policy, and 74% of participants completely skipped the privacy policy via "quick join" click-wrap.

89. *Id.*

90. *See* Solove, *supra* note 9, at 1881.

91. Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ [https://perma.cc/93FW-EEPA].

92. M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1054 (2013), https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1020&context=ndlr. Information overload is a classic example of shared cognitive biases.

93. *See* Solove, *supra* note 9, at 1883.

94. Marie C. Pollio, *The Inadequacy of HIPAA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding*, 60 N.Y.U. ANN. SURV. AM. L. 579, 601–04 (2004).

95. Calo, *supra* note 92, at 1035 n.47 (quoting Howard Latin, *"Good" Warnings, Bad Products, and Cognitive Limitations*, 41 UCLA L. REV. 1193, 1215–20 (1994)), 1054.

detail, there is less time to read. The privacy community has responded to this challenge with an increased focus on layered privacy policies, where individuals can click on truncated areas of a primary notice to read more information about specific privacy practices.[96]

Traditional health care benefits from the context provided in a doctor-patient relationship. If a patient is concerned about information use, the individual can ask a question in the environment and likely has an opportunity to do so. When a patient checks into a clinic, the Notice of Privacy Practices is provided, and the patient has an opportunity to ask questions, should they so choose. Certainly, choice in traditional health care could improve, but the HIPAA model is better designed for a face-to-face interaction than for IoHT. For non-traditional health care, such as IoHT and health apps, individuals generally do not benefit from the built-in context or assistance a traditional health care environment might have. Rather, consumers are expected to derive any context from their interaction with a computer screen.

Under some circumstances, when a patient is providing voluntary consent under HIPAA then later signing authorization forms, the patient may not clearly understand the difference. In these cases, the patient likely relies on the doctor as a fiduciary to explain this information fully. The patient also may not understand that HIPAA only covers certain entities and relationships and may feel a false sense of security for this reason, as well, a misplaced trust in the law for other health technologies, such as IoHT devices or other health applications.

Consider individuals engaging in typical technology situations: an individual wants to use a health app recommended by a doctor, a connected insulin pump, a telehealth system, a connected scale, and a steps tracking device. Assuming each of these are reimbursable through insurance, each of these applications would require its own authorization form for the doctor to share medical information with these companies. Each time every company changes their data handling activities even in a limited way, such as engaging a new third-party technology supplier or the authorization term expires, these companies would likely need to execute another authorization. For those that are not reimbursable, they are not likely subject to HIPAA and fall to FTC broad oversight, with little to no specific requirements, except for the Fair Information Practices.[97] In the past, an authorization was typically used for face-to-face activities; today, a paper

96. Mehmet Munur, Sarah Branam & Matt Mrkobrad, *Best Practices in Drafting Plain-Language and Layered Privacy Policies*, INT'L ASS'N PRIVACY PROFS. (Sept. 13, 2002), https://iapp.org/news/a/2012-09-13-best-practicesin-drafting-plain-language-and-layered-privacy/ [https://perma.cc/2B9S-S6VV].

97. *See supra* Part I.B.5 and accompanying notes.

model is being used for digital relationships, which have become more numerous in number, more attenuated in relationship, and more ubiquitous in our lives.[98]

4. Consent Myth 4: Consumers Can Actively Represent Their Interests through Smart Reading of Privacy Policies and "Informed" Consent (Exogeneity Problem)

Privacy advocates have focused on solving the first three consent problems by developing privacy policies that anticipate reading issues and more effectively manage time commitments. The FTC has advocated for "just-in-time" notice and consent.[99] Although these developments have improved privacy policy contents and display, the model has not necessarily improved actual choice, for the reasons just described. Furthermore, some aspects of information handling simply cannot be communicated effectively to appropriately advise of downstream risks.

Although information asymmetry plays a role in effective communication, in some cases the organization, which is providing computerized notice to which consumers consent on IoHT devices, does not clearly understand its own information handling practices. While it is possible to envisage improved disclosures, the issue with exogeneity is not necessarily one of communication; rather, it is an issue of organizational self-knowledge. Because organizations do not understand their own technology practices, organizations craft privacy notices with basic information, relying on the consumer to make an "informed choice" based on imperfect information, when most consumers are not privacy experts.[100] In many cases, even privacy experts cannot understand a privacy policy's contents.[101] Studies have shown that Americans may be willing to negotiate over personal information, but first, they want to understand how good the deal is and what risks they might face.[102] If organizations can effectively communicate risks, individuals may be more likely to truly "choose" a path that not only advances individual autonomy but also satisfies commercial goals.[103]

---

98. *See supra* Part III and accompanying notes.

99. *See* FTC 2010, *supra* note 63, at vi.

100. Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 77 (2018).

101. *Id.* at 77 n.9.

102. Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RES. CTR (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacyand-information-sharing/ [https://perma.cc/G6NS-DM98].

103. Although not discussed within this paper, while individuals often do not have a choice upfront, they often are unable to protect themselves through the legal system either, and are instead reliant on administrative agencies. Lack of individual civil recovery further minimizes an individual's choice with respect to the model overall. An individual is first expected to agree without bargaining,

Making choices about what data will be collected and how organizations might manage data downstream is probably the most challenging information for an individual to receive, understand, and accurately ascertain potential risk. Unlike other types of personal information, health data can contain directly sensitive information or proxies for sensitive information, and when data are exchanged, duplicated, or stored by a third party, these activities may increase the potential volume that could be misused or compromised.[104] Furthermore, health data can easily be sold on the black market, netting $10–50 per record, especially insurance information often collected by CEs and shared with BAs for purposes of processing.[105] Although other health organizations may not collect insurance information, health data collected can help to perpetuate fraud by providing information used to validate accounts or prove identity. For health data, advising of downstream risks becomes a more critical step. However, instead of focusing on advising the individual, in these cases, the law (where it applies) has directly regulated organizations. This degree of regulation has not effectively reduced privacy issues for health data. Data breaches, for example, continue to increase in frequency.[106]

The use of third parties, especially for services, has simultaneously decreased cost while increasing exogeneity issues.[107] Third party activities are generally secured via contract, whether formally under HIPAA as a BA, or other agreement, usually a Master Services Agreement. Third parties often use third parties, which in turn may use third parties, and so forth.[108]

---

then to navigate a sea of privacy policies, followed by difficult to understand language and almost unforeseeable risks of which the individual is not advised. Finally, the individual has no private right of action under most models that regulate bad behavior. Under some state UDAP laws, an individual may have a right of action, or the attorney general may create a fund for aggrieved consumers. However, under the primary federal laws, HIPAA and the FTC Act, individuals do not have an individual right of action. Further, it is still extremely difficult to prove injury in tort or contract, for privacy or security issues, so the common law does not provide much of an alternative avenue.

104. Roger Allan Ford & W. Nicholson Price II, *Privacy and Accountability in Black-box Medicine*, 23 MICH. TELECOMM. & TECH. L. REV. 1, 5 (2016); Scott Rupp, *Why Do Hackers Want Medical Records?,* ELECTRONIC HEALTH REP. (Apr. 18, 2018), http://electronichealthreporter.com/hackers-wantmedical-records/ [https://perma.cc/69XC-UJMM].

105. *Id.*; Caroline Humer & Jim Finkle, *Your Medical Record Is Worth More to Hackers Than Your Credit Card*, REUTERS (Sept. 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 [https://perma.cc/9SEP-UYZ9].

106. Rachel Z. Arndt, *Healthcare Data Breaches Caused by Hacks Are on the Rise*, MODERN HEALTHCARE (Aug. 18, 2017), https://www.modernhealthcare.com/article/20170816/NEWS/170819925 [https://perma.cc/H2SK-UM8Y].

107. Third parties are generally not transparent to consumers under most circumstances. In some cases, confidentiality obligations limit organizations sharing who their third parties are.

108. A particularly curious situation is when a Third-Party A (TP-A) is in a relationship with the primary party (that provides service or product to a consumer), and TP-A uses a third party, TP-B, that uses another third party, TP-A, which happens to be the same third party in the primary relationship. The contractual provisions between the primary party and TP-A may have radically different provisions,

In "sub-privity," none of these third parties likely has a direct relationship with the organization that provides service or contracts directly to the consumer.[109] This means that the consumer, and sometimes the organization with which the consumer does business, does not have visibility to data location or handling procedures. Relationships subject to sub-privity likely suffer from greater exogeneity issues, which may also complicate recovery in breach of contract, as privacy or indemnification language may differ from contract to contract.[110] When organizations may not be able to trace third-party data handling beyond the first or second third parties, it is unlikely that consumers will understand these intricacies or be able to reasonably enforce their own interests simply from reading a privacy notice.[111]

5. Consent Myth 5: Current Models for Notice and Consent Are Applicable to New Technology (Temporal Problem)

Technology has made the traditional consent model almost impossible to facilitate. Although specific health care activities enjoy some benefits of layered privacy protection under U.S. law, health technology of the future complicates both how organizations facilitate consent and the degree to which individuals benefit from fulfillment of existing requirements. Connected and distributed environments, designed to reduce costs and improve health outcomes, increase the frequency with which product and service uses can change, while simultaneously making it much more difficult to effectively inform consumers about privacy practices and potential risks.

New technologies complicate traditional notice and consent models by frustrating the prior information aspect of "*informed consent,"* which incorporates a temporal requirement—for consent to be enforceable, notice of data collection and use practices must be communicated first.[112] Temporal limitations, or the requirement to notify and receive consent before data collection or use, may be impossible to facilitate with some

---

including privacy provisions in the contract between TP-B and TP-A. *See* CHARLOTTE A. TSCHIDER, INTERNATIONAL CYBERSECURITY AND PRIVACY LAW IN PRACTICE 382 (2018).

109. *Id.* at 378 n.299, 381–82. Exporting or subcontracting data in this way can create cost savings, though often at the expense of the individual, who has no idea where her data might be or with whom.

110. *Id.*

111. *Id.*

112. The informed consent model borrows the concept from clinical trials, where informed consent involves providing information to a trial participant that reasonably appraises the participant of potential risks before the participant consents to the trial. *See* Dalar Shahnazarian, Jennifer Hagemann, Monica Aburto & Susan Rose, *Informed Consent in Human Subjects Research*, OFF. PROTECTION RES. SUBJECTS 1, 3–5 (2013), https://oprs.usc.edu/files/2017/04/Informed-Consent-Booklet-4.4.13.pdf [https://perma.cc/D9TD-7FW6].

technologies or tremendously impractical for other services. The frequency with which new notice and consent is required (i.e., upon material change) may further exacerbate structural and cognition problems, while simultaneously reducing organizational efficiencies.

The IoHT has introduced wearables, implantable devices, affixed devices, and apps that connect to the Internet, promising reduced health care costs and consumer convenience.[113] The backbone of IoHT includes big data, which often provides more effective services in IoHT from more substantial data collection.[114] IoHT and other health applications, apps, and surgical equipment have begun to include AI capabilities.[115]

Increasingly, health applications with AI apply machine learning utilities to facilitate self-learning models that reduce time and effort while increasing predictability and reliability. IoHT systems create *and* consume incredibly large data volumes.[116] Machine learning utilities require big data for reliable, correct results; machine learning without big data produces predictably incorrect results.[117] Unsupervised machine learning utilities often use data in unpredictable ways to create the algorithms on which the machine learning utility runs.[118] Uniquely, these utilities create these algorithms from the data itself—by using computing power to find patterns amongst data, rather than superimposing a pattern on the data.[119] The results could transform healthcare: with a big data backbone, AI could turn the world into a clinical trial, so long as AI can run on a big data database.[120] However, big data, and the technologies consuming its products, tend to run at cross-purposes with privacy from a collection perspective. AI, IoT, and

113. ACCENTURE 2017 INTERNET OF HEALTH THINGS SURVEY, https://www.accenture.com/t20180423T065104Z__w__/us-en/_acnmedia/PDF-42/Accenture-Health-2017-Internet-of-Health-Things-Survey.pdf#zoom=50 [https://perma.cc/XES2-Y5K6] (last visited March 5, 2019).

114. Avantika Monnappa, *How Big Data Is Powering the Internet of Things (IoT) Revolution*, SIMPLILEARN (Sept. 11, 2017), https://www.simplilearn.com/how-big-data-powering-internet-of-things-iot-revolution-article [https://perma.cc/PH4Q-367D].

115. David Kaplan, *The 'Internet of Health Things' To Be Worth $163 Billion By 2020*, GEOMARKETING (Apr. 21, 2017), https://geomarketing.com/internet-of-health-things-worth [https://perma.cc/E3WJ-4PZX].

116. Tom Krazit, *The Internet of Things Will Make Big Data Look Small,* FORTUNE (Mar. 3, 2016), http://fortune.com/2016/03/03/internet-data-structure/ [https://perma.cc/53DE-4SNL]; Tamara Dull, *Big Data and the Internet of Things: Two Sides of the Same Coin?*, SAS, https://www.sas.com/en_us/insights/articles/big-data/big-data-and-iot-two-sides-of-the-same-coin.html [https://perma.cc/N2A3-5BFT] (last visited Mar. 5, 2019).

117. Bernard Marr, *Why AI Would Be Nothing without Big Data*, FORBES (June 9, 2017), https://www.forbes.com/sites/bernardmarr/2017/06/09/why-ai-would-be-nothing-without-big-data/#6aaf83764f6d [https://perma.cc/LXL2-AQ4G].

118. Cade Metz, *Building A.I. That Can Build A.I.*, N.Y. TIMES (Nov. 5, 2017), https://www.nytimes.com/2017/11/05/technology/machine-learning-artificial-intelligence-ai.html [https://perma.cc/JT9Y-5M7H].

119. *Id.*

120. *The Power of AI to Transform Clinical Trials*, ICON (Apr. 11, 2018), https://www.iconplc.com/insights/blog/2018/05/18/the-power-of-ai-to-transform-clinical-trials/ [https://perma.cc/5RSJ-999B].

big data seek to maximize collection, rather than minimize it, to the benefit of the patient and the organization.[121]

The Consent Myth consists of five major problems that, considered holistically, render consent a choice that does not protect individual autonomy. These problems illustrate that the predominant privacy model cannot, in its current conception, effectively advance privacy interests, especially in the health sector.

IV. PRINCIPLES OF A "CHOICE-FIRST" PRIVACY MODEL

So how might organizations solve these complex problems? A "Choice-First" Model considers the bargaining position of the consumer in relation to an organization, a model based on the expectations of an ongoing relationship rather than a one-time, transactional relationship. The Choice-First Model places the consumer, an individual, as the central focus. With recognition of an ongoing relationship oriented within an ever-evolving and changing contextual environment, orienting a model towards an ongoing relationship both reinforces multiple opportunities to gather more information, make choices, and build trust.

A Choice-First Model may be implemented differently depending on the circumstances. However, certain principles, designed to combat existing problems, should both advance individual interests and account for some degree of organizational flexibility. Due to substantial existing privacy problems that erode autonomy, at least initially a Choice-First Model may appear restrictive for less-regulated organizations, such as those only under the FTC's purview, but may better fit new technology models than existing HIPAA regulation.[122]

A. Principle 1: Initiating Service Should Be Non-Coercive

Within the health care sector and other sectors, consumers who initially form a relationship with an organization have a specific purpose for that relationship: they want a product or service. Although this moment may provide an opportunity for organizations to capitalize on consumer interest by gathering permission for additional uses, bundling secondary uses with primary uses creates a high likelihood for coercion. Non-HIPAA-regulated organizations often bundle consent to use data required for a service or product to function with other desirable or lucrative data not required for

121. *See* Ford & Price, *supra* note 104, at 24–25.

122. *See supra* Part I.E and accompanying notes. Please note: This section intends to further the dialogue about an effective policy model, rather than specifically defining how HIPAA or FTC practices might change to introduce this model.

the service.[123] Although substantively these secondary uses may not be considered substantively coercive, the act of bundling itself could be considered a more coercive practice.

When an organization only bargains for data central to the service or product's purpose, primary use, a consumer benefits from the immediate context of the information provided: data collected will be foreseeable and generally reasonable, because data are necessary for the service or product to function properly. For example, if a consumer signs up for a health tracker that monitors diet, steps per day, weight, and blood sugar values; it will likely be foreseeable that the organization will need access to health information and activity levels for purposes of storing the data or offering online coaching and reminders. If the steps-per-day feature includes a map that records steps on a geographic map, it is reasonably foreseeable that the organization captures geolocation data.

Other benefits to this type of model include length and audience appropriateness: it is far easier to write privacy policies that account for fewer uses and adapt this communication for the audience. Initial notice could be improved, for example by including more active, emotionally rich language, "visceral language," which more persuasively advise risks.[124] Organizations could also tailor notices to specific user groups to make them more understandable and engaging or provide different models for sophisticated parties.[125]

The marketplace will also benefit by reducing administrative tasks associated with commencing service. Instead of an organization being responsible for gathering consent and managing associated workflows and records, consent may not be necessary. When data sharing is based on the acquisition of a product and data shared is reasonably foreseeable to the consumer, the notice functions as a reminder, rather than the primary communication vehicle. Instead, the context of the initial transaction itself and the nature of the product or service provides the framework for understanding what data will be collected and under what circumstances.[126] Organizations can amplify understanding by clearly describing data collection as part of marketing materials related to features or functions.

123. Bundled consent leads to reduced understanding of data handling practices, extends the length of privacy policies, and can lead to an individual giving up much more than she might otherwise, due to the adhesive nature of the agreement.

124. *See* Calo, *supra* note 92, at 1035, 1045.

125. *Id.* at 1041 (describing Hanson & Kysar's population segmentation study), 1062 (citing Berin Szoka).

126. This model echoes a similar sense of context and foreseeability under the European Union's legal bases: data sharing pursuant to a contract where such sharing is reasonably foreseeable does not require consent. *See* The General Data Protection Regulation (EU) 2016/679 Art. 6 (1)(b). Although often the EU is considered substantially more restrictive than the United States, multiple legal bases for data collection and use are legitimate, other than consent.

This model is consistent with HIPAA requirements and works as intended: most individuals in a medical office, for example, likely do not need to read the Notice of Privacy Practices, although they have an opportunity to do so. Primary use would involve providing a privacy notice but limiting its contents to only uses that a reasonable person would expect, such as data collection central to a system's functionality. For example, a FitBit-like device that monitors healthy behaviors would likely gather information about steps, dietary information, and geolocation data for purposes of providing the FitBit service and fulfilling marketing commitments. However, an individual's mobile device contacts list might be outside what an individual would expect. Because primary use is reasonably expected, consent need not be required: simply using the device demonstrates implicit consent. Although the Fair Information Practices might recommend employing consent, a model for primary uses without consent would create greater consistency for both HIPAA-regulated and non-HIPAA-regulated organizations.

B. Principle 2: Additional Uses Must Be Informatively Communicated and Require Explicit Consent

Secondary uses of personal information or additional data collection have a higher potential for abuse. Further, consumers may be less likely to understand the ramifications of uses that extend beyond an immediate product or service. For this reason, secondary uses should require sufficiently educational communications that enable a consumer to better understand risks to her prior to consenting.[127] One way to contextualize these exchanges is to call them a "proposal," or other language that signals an invitation to bargain rather than an obligation to disclose.

Specific proposals should be highly specific, not misleading, and should contain: 1) the specific use or category of uses proposed (e.g., marketing materials sent to your email address), 2) the data targeted and why the organization wants these data elements (their value), and 3) detailed risks associated with sharing these data. Each proposal should be displayed one at a time to focus attention. After a consumer makes a decision, the system should not display the exact same proposal to solicit consent again in a manner to irritate or attempt to coerce the individual to change her mind. These proposals should be displayed after the individual has already

127. The Author would like to note that consent can perform an important function when the individual consenting has been truly provided the opportunity and appropriate information to make a decision in her own best interest. Consent procedures are not problematic, but the circumstances under which consent is given generally are, as is using consent as a legally defensible proxy for choice.

initiated the service, and not as part of the service initiation workflow or bundled with the primary use notice.

In this model, the individual has already received the service and therefore is under no actual or perceived requirement to agree to share more information than she is comfortable. Further, proposals regarding the data's business value juxtaposes data *wanted* (secondary use data) with data needed (primary use data), which reduces power imbalances between the consumer and the organization. This model reinforces the exchange of promises and consideration.[128]

Finally, organizations should communicate a risk advisory and use real examples that help an individual contextualize a potential downstream risk. See an example proposal below:

> The HeartMonitor Lite measures your heart rate through vibrations. We would like to share your heart rate data and other data collected through your passive use of this device (including GPS data) with our partners, who develop pharmaceuticals. We will receive a financial benefit for these data. Although we contractually bind our partners to a contract with us, we cannot guarantee the same privacy or security protections you receive from us. Do you consent to share these data with our partners? (Yes/No/More Information)

This example is written with the intention of giving an individual appropriate information pertinent to her decision, such as the organization's financial interest in the data and potential risks to the individual. A proposal could be coupled with a financial or other incentive for providing this information, such as access to other functionality or direct payment, although for more sensitive data use, financial compensation could be prohibited.[129] Although this does create a market for information to some extent, the individual can make a choice, rather than being duped into sharing data that nevertheless benefit the organization. Furthermore, other

---

128. It should be noted that of course, a bargain and exchange model does potentially have a higher impact on individuals at a lower income level, as they may not be able to afford privacy. However, in this model, rather than "buying back" privacy, the individual can choose whether their information is worth the additional service or financial benefit and opt-into these practices.

129. It is hard to imagine collecting data from an insulin pump or pacemaker customer for profit, yet data has substantial value, often for purposes that ultimately will improve human health. Data set purchasing for, for example, artificial intelligence systems has increased substantially as technology requires greater data volume to spur innovation. As Danielle Citron aptly pointed out to this author, it is difficult to imagine that someone reliant on technology should be selling access to the information produced through its usage. For this reason, the United States could consider some limitations on secondary use, although this will reduce the overall usefulness of these data. *See* Morris Panner, *Health Data Meets Artificial Intelligence and Machine Learning*, FORBES (NOV. 21, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/11/21/health-data-meets-artificial-intelligence-and-machine-learning/#740bbe8cc62d [https://perma.cc/D44Q-9P2H]. However, sensitive data could be limited to philanthropic donation.

social benefits could also result, including better or more effective technologies that can improve human health.

HIPAA authorization, to some degree, uses specific communication about data type and associated uses, although information about financial interests and risks are not usually disclosed. Further, HIPAA authorizations require a level of specificity that would not likely be compatible with less defined purposes, such as data collection for AI use. See an example proposal below:

> Your Daily Health Service uses lifestyle information entered by you and gathered through wearing the Daily Health bracelet to predict a personalized plan for improving your health. We would like to use your lifestyle information to improve the service for all users by combining your data with the data of other users. This prediction model uses artificial intelligence and we cannot always predict how or for what purposes your data might be used. We remove some identifying data, but the data remaining could be enough data to identify you. Do you consent to share these data for use in our AI system? (Yes/No/More Information)

This example might not be able to qualify for a legal authorization under HIPAA, as the data uses and details are not highly specific. If HHS wants to support new technologies like AI, it might consider permitting broader, less-specific use disclosures for organizations creating AI utilities.[130] HHS could use a similar model to its analysis of data for future research data uses as a starting point.[131] Organizations involved in AI activities could secure authorization so long as they have an internal Institutional Review Board (IRB), or an advisory board tasked with evaluating clinical study ethics and human subject safety, specifically defined for AI activities to anticipate potential ethical or safety issues and undergo regular Privacy Impact Assessments (PIAs) or audits. For example, the IRB could engage an expert outside firm to examine testing, machine learning training approaches, or question the utility of collected data for ongoing AI uses.

Of course, organizations may desire to incentivize consumers to share additional data for other purposes.[132] In other cases, secondary uses may be

130. *See supra* Part I and accompanying notes.

131. *See supra* Part I and accompanying notes.

132. When organizations desire to collect additional data, they may engage in some contracting process. *See generally* Jake Linford, *Unilateral Reordering in the Reel World*, 88 WASH. L. REV. 1395 (2013) (describing how contract formation has shifted from a negotiation model to contracts formed without negotiation at arm's length, and this has intensified issues with meaningful consent). Information exchange relationships could employ multiple models, unilateral and negotiation-based, to selectively engage patients or consumers in the bargaining process.

intrinsically reasonable, such as health data for research purposes.[133] However, organizations will likely want to use previously collected personal data for other (often commercial) purposes. However, instead of gathering such data through techniques that hide the true motivation for data collection and leave consumers without the full picture, organizations can use these models to transparently propose new bargains to consumers. More frequently, organizations have begun to incentivize data sharing with coupons or additional services. When consumers have accurate, pertinent information, they are comparatively better positioned to advocate for their respective interests. Unlike a contract of adhesion, discrete bargaining of this kind reduces information asymmetries.

Organizations should require explicit consent when agreeing to proposals that involve the collection or use of personal information.[134] Because secondary uses are not reasonably foreseeable and potentially could introduce greater risk to the individual due to their exogeneity, explicit consent when combined with appropriate information would dually ensure an individual intends to share data in this way and protect organizations using these data.

C. Principle 3: Address User-Centric Needs with UI-Based Controls and User Preferences

A Choice-First Model should not only involve discrete exchanges at the beginning of a relationship: individuals should be able to make decisions throughout an ongoing relationship with an organization. Privacy should be part of most interactions and workflow within a User Interface (UI). User Experience (UX) engineers, used for a variety of purposes in industry, have analyzed the mental models individuals bring to business processes, products, and digital interfaces.[135] Integrating choices into each workflow not only illustrates a commitment to strong design, it also reflects an

133. *See generally,* W. Nicholson Price II, *Drug Approval in a Learning Health System*, 102 MINN. L. REV. 2413 (2018) (describing the value of personal information for purposes of drug development).

134. Of course, a question still remains as to the availability of consent revocation when secondary uses are considered part of an agreement. I would recommend an alternative to the current revocation of authorization model under HIPAA—a limited prohibition model. When organizations and consumers bargain for access to information, it is reasonable that an organization should see the benefits, as should consumers. For this reason, I would suggest a *reasonable* bar on consent revocation for a period of time. This could be specified within the Proposal or established by administrative interpretation, such as a cap of ninety days before any data collected must be rendered de-identified and no longer used in original form.

135. *See, e.g.*, ACCENTURE 2017 INTERNET OF HEALTH THINGS SURVEY, *supra* note 113; Kovila P.L. Coopamootoo & Thomas Groß, *Mental Models: An Approach to Identify Privacy Concern and Behavior*, SYMP. ON USABLE PRIVACY AND SECURITY (SOUPS) 2014 2, https://cups.cs.cmu.edu/soups/2014/workshops/privacy/s2p2.pdf [https://perma.cc/RV9G-4PEP].

understanding that individuals benefit from context for making decisions about their privacy. If choice is a central requirement for human autonomy, choice should be built into a system, intrinsic to UI functionality, with appropriate information available at precise moments.

Workflow-based privacy controls put the power of choosing which information to share and under what circumstances into the hands of an individual. Work-flow based privacy controls usually involve 1) integrated, use-case controls and 2) settings-based preference management.[136] Settings-based preference management allow for an individual to make "just in time" choices about previous decisions, such as whether to share photos with an organization, whether a profile is public or private, or when an individual shares information with a health care provider. Consider the following scenario:

> Serge has an online account that tracks his seizure frequency from an implantable brain stimulator that is equipped with wireless connectivity. The data passes to a backend system where it is aggregated, analyzed, and displayed on a mobile app. When looking at the results, Serge notices a higher frequency this month than he has in months past. In the interface, there is a Send to Dr. button with a Mail icon. When he clicks Send, it opens an email record, appends the data report, displays the last neurologist's e-mail address, and sends to Serge's neurologist. Serge has an opportunity to look at the button and change his mind or otherwise change his neurologist.

While use-case controls tie to specific actual tasks within a site, settings group preferences together for easy access and change. Preferences may include detailed options but benefit from top-level simplicity. Preferences most clearly tie to broad decisions rather than highly contextual ones (e.g., an individual wanting to view previously collected personal information for purposes of determining that such information is accurate). Under HIPAA, applicable entities must provide access to data and facilitate portability requests. Other requests that merit consideration include risk-minimizing requests, such as consent revocation with blocking or compulsory de-identification.[137]

---

136. The term "control" used here is meant to denote specific settings or interactive features which enable an individual to make decisions about what data are shared and with whom.

137. Consent revocation with blocking simply stops automated systems from continuing to proliferate personal information through recurring processes. Compulsory de-identification has not been discussed much to-date, but it could provide an alternative option to data erasure, which may reduce data volume for technologies dependent upon those data. Compulsory de-identification could be initiated by the individual. If the United States decided this could be an option for better overall individual choice, organizations should have a clear view of appropriate standards for de-identification, other than the HIPAA De-Identification Safe Harbor.

D. Principle 4: The Better-Positioned Party Should Manage Exogenous Privacy Risks

Exogenous privacy risks generally result from either lack of effective information and practices required for a consumer to make an autonomous choice or information about business practices that are unavailable to an individual. Organizations can address the first circumstance by focusing on Principles 1–3. However, the second requires special consideration. These business practices usually are confidential and not immediately apparent from the perspective of the individual. For example, a consumer may not know that a Website is displayed from a cloud provider in Indonesia or that a contract group handles health care insurance claims.

Although Principles 1–3 position the individual in the center of the Choice-First Model, for exogenous data such as technology infrastructure types or third parties engaged, the model must rely on organizations making these choices for three reasons: 1) Organizations routinely make technology and third-party choices in the normal course of business, are reasonably sophisticated with respect to third-party contracting, and should be responsible for corresponding risks as a party to the contract; 2) Organizations are comparatively better positioned to manage exogenous risks on behalf of users due to both their contract status and their operational and legal proximity to third parties; and 3) Technology and service choices usually apply to all individuals as a group (not specific individuals), rending third-party management a collective endeavor.

From a risk management perspective, organizations should manage third-party risk by conducting regular assessments and drafting and enforcing contractual commitments. However, at least some transparency could enable effective privacy self-management for engaged individuals. A relatively simple way to support self-management is to permit requests for information. For example, organizations should be required to retain a named list of third parties pertinent to the information collected, used, transferred, or stored. Links should be provided to these third parties' privacy policies, if not consistent with the primary organization. Organizations could provide additional context, such as the rationale behind using these third parties or what they do on behalf of the organization.

CONCLUSION

A choice-first privacy model enables an individual to make discretionary, contextual decisions about their personal information in a prior and continuous model. Within this model, an individual will be less burdened by reasonably predictable data uses while dynamically engaged in

bargaining over less predictable data uses. Because primary and secondary data uses are not bundled under one privacy notice, individuals can choose to forego additional data collection and use, if desired. Further, when individuals can self-manage in a context-specific manner, they are better able to make discrete decisions about their data at a point in time, enabling decision-making that is likely clearer to the individual. Finally, when organizations are directly responsible for risk factors exogenous to the individual, organizations cannot pass on the responsibility to individuals who are not able to fully ascertain such risk.

The increasingly pervasive interaction between private and public spheres continues to complicate individuals' privacy interests, especially for connected health technologies like the IoHT. Although perfect choice might be illusory or at least aspirational, the potential for less abusive practices and enhanced choice in human-computer contexts might be possible. By confronting our misconceptions about consent, the United States will be better able to consider more effective models for individual choice that enhance, rather than hinder, individual autonomy.