WEARABLE AI, BYSTANDER NOTICE, AND THE QUESTION OF PRIVACY FRICTIONS

ZAHRA TAKHSHID[*]

ABSTRACT

With the rapid advancement of Artificial Intelligence ("AI") technology and the widespread availability of large language models ("LLMs"), wearable AI devices and designs for new hardware have surged like never before. While wearable AI was traditionally marketed for health and fitness purposes, many of the emerging products are multifunctional. These features can jeopardize the privacy of bystanders in addition to consumers. Product designers are thus facing a dilemma: ensuring third-party privacy or guaranteeing convenience and a user-friendly design. This Article argues for mandating "privacy frictions" to function as bystander notice and consent for wearable AI devices with audiovisual recording capabilities. Privacy frictions are tangible measures that can put the reasonable bystander on notice. While this human-centered privacy design may impact the users' experience, it ensures a future where privacy continues to be relevant and valued.

[*] Assistant Professor of Law, University of Denver Sturm College of Law and Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University. For helpful comments, I am grateful to Boston University's Information Privacy Law at the Crossroads Symposium, Bernard Chao, and Viva Moffat. Thanks to Carolyn Payne for excellent research assistance.

CONTENTS

INTRODUCTION

During one of the spring and summer fashion shows of 2024 in Paris, models were showcasing not just clothing, but also a wearable Artificial Intelligence ("AI") device called the Ai Pin.[1] The clothing-based wearable was launched by Humane, a company founded by former Apple executives.[2] It was introduced as a "personal consumer technology" that "harness[es] the full power of artificial intelligence."[3] The screenless device does many things, from simple tasks like making calls and taking photos, to more complicated tasks, such as acting as a personal assistant powered in part by ChatGPT.[4] With a forward-facing small camera on the device, the company emphasized its commitment "to building a future where AI seamlessly integrates into *every aspect* of our lives."[5] Another wearable AI project, called the Rewind Pendant, is a necklace "that captures what you say and hear in the real world and then transcribes, encrypts, and stores it entirely locally on your phone."[6]

These are just two examples of a new wave of wearable AI products.[7] While wearable AI has been around for years, it has traditionally been marketed for its use in the health and fitness industries and corresponding personal use.[8] At the time, data privacy concerns were about personal choices of the end user and their interaction with the devices.[9] However, what is distinct about the new surge of AI hardware is the overwhelming interaction of the devices with

[1] *Humane Reveals First AI Device - the Ai Pin - at Coperni's Paris Fashion Show Ahead of Full Unveiling on November 9*, HUMANE (Sept. 29, 2023), https://hu.ma.ne/media/humanexcoperni [https://perma.cc/3GF6-SBCT].

[2] Humane was founded by the husband-wife team of Imran Chaudhri and Bethany Bongiorno, former Apple executives who left in 2016. Aaron Tilley, *Can an AI Device Replace the Smartphone?*, WALL ST. J. (Nov. 9, 2023, 12:00 PM), https://www.wsj.com/tech/ai/humane-ai-pin-3311391e.

[3] *Humane Launches Ai Pin*, HUMANE (Nov. 9, 2023), https://hu.ma.ne/media/humane-launches-ai-pin [https://perma.cc/AY8Y-N2GY].

[4] Tilley, *supra* note 2.

[5] *Humane Launches Ai Pin*, *supra* note 3 (emphasis added).

[6] *Introducing Rewind Pendant*, REWIND AI, https://www.rewind.ai/pendant [https://perma.cc/3LYR-4L86] (last visited May 14, 2024). The product has not yet been launched. *Id.*

[7] There are other AI devices either under development or being launched. *See, e.g.*, *Rabbit R1*, RABBIT, https://www.rabbit.tech/rabbit-r1 [https://perma.cc/3ZJS-2WAR] (last visited May 14, 2024) (highlighting "pocket companion" that can access all your apps with its built in AI assistance and comes with microphone and camera). For a review of the product, see Lisa Eadicicco, *Meet Rabbit R1: A Petite Orange Box Redefining App Usage with AI Assistance*, CNET (Jan. 20, 2024, 6:00 AM), https://www.cnet.com/tech/mobile/meet-rabbit-r1-petite-orange-box-redefining-app-usage-ai-assistance/ [https://perma.cc/Z8E5-95ZS].

[8] Nicole Chauriye, *Wearable Devices as Admissible Evidence: Technology Is Killing Our Opportunities To Lie*, 24 CATH. U. J.L. & TECH. 495, 495 (2016).

[9] *See* Terence M. Durkin, *Health Data Privacy and Security in the Age of Wearable Tech: Privacy and Security Concerns for the NFLPA and Whoop*, 19 J. HIGH TECH. L. 279, 279 (2019).

their surroundings, and thus bystanders—people who do not personally use the product but whose privacy is nevertheless jeopardized.[10]

The wearable AI industry has paid little attention to third-party privacy, with most of the work focusing on user privacy and attaining user consent.[11] A bystander is the person who is not using or wearing the AI device but either knowingly or unknowingly interacts with the product, or is a subject about which the device seeks information—not someone who has an incidental presence.[12] One early example of such privacy implications involved Google Glass Enterprise.[13] The wearable glasses "allow[ed] users to access the Internet, take photos and film short snippets."[14] The privacy challenges that

[10] *See* Suchismita Pahi & Calli Schroeder, *Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy Is Several of Them*, 4 NOTRE DAME J. ON EMERGING TECHS. 1, 3-4 (2023).

[11] *See, e.g.*, Justin Evans & Katelyn Ringrose, *From Fitbits to Pacemakers: Protecting Consumer Privacy and Security in the Healthtech Age*, 68 CLEV. ST. L. REV. ET CETERA 1, 1 (2019) (discussing benefits of wearable devices in healthcare industry and identifying areas where privacy and data security could be improved); Kenny Gutierrez, *Privacy in Wearables: Innovation, Regulation, or Neither*, 13 HASTINGS SCI. & TECH. L.J. 21, 25 (2022) (examining privacy concerns about wearable technology and user consent requirements under different sectoral privacy laws); Michael Guihot, Anne F. Matthew & Nicolas P. Suzor, *Nudging Robots: Innovative Solutions To Regulate Artificial Intelligence*, 20 VAND. J. ENT. & TECH. L. 385, 445-54 (2017) (proposing solutions for regulating development of AI, including privacy concerns); Janice Phaik Lin Goh, *Privacy, Security, and Wearable Technology*, LANDSLIDE, Nov.-Dec. 2015, at 30, 31 (discussing challenges to traditional privacy principles wearables present, i.e., principles of notice and choice); Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH., Feb. 2015, at 1, 1-3 (noting privacy concerns about wearable technology but "encourag[ing] policymakers to allow [it] to develop in a relatively unabated fashion").

[12] The bystander in this Article is not the person some have referred to as the "bycatch." The bycatch is the incidental target. *See* Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555, 567-68 (2020) ("Bob may be a bystander in a photograph taken of Alice, in which the photographer has no real intent to capture Bob's image. . . . Bycatch can also occur when Alice and Bob share physical space."). The bystander here is intentionally the target of the device's data collection, whether the bystander interacts with the device intentionally or inadvertently.

[13] David Streitfeld, *Google Glass Picks Up Early Signal: Keep Out*, N.Y. TIMES (May 6, 2013), https://www.nytimes.com/2013/05/07/technology/personaltech/google-glass-picks-up-early-signal-keep-out.html. Although Google Glass continued to be present in the healthcare industry after it was discontinued, Google halted software updates on September 15, 2023 and warned that the app may stop working any time after that date. *See* Nicolas P. Terry, Chad S. Priest & Paul P. Szotek, *Google Glass and Health Care: Initial Legal and Ethical Questions*, 8 J. HEALTH & LIFE SCIS. L. 93, 95 (2015); Mitchell Clark, *Google Glass Enterprise Edition Is No More*, VERGE (Mar. 15, 2023, 5:28 PM), https://www.theverge.com/2023/3/15/23641872/google-glass-enterprise-edition-discontinued-support [https://perma.cc/5CF2-EBHB].

[14] Streitfeld, *supra* note 13.

were raised, with some calling it "creepy,"[15] in part caused the discontinuation of the product. Yet the new wave of wearable AI devices, including Meta's smart glasses,[16] share many of the same privacy concerns as Google Glass, but with one major difference: they are here to stay.

Clearview AI is also working on $999 glasses that allow "the wearer to look at a stranger from as far as ten feet away and find out who they [are]."[17] While the product is currently being pitched for military use,[18] one can easily imagine a future where it is also sold to the general public. Such level of detection is scary. It gives power to those who have the wearable AI over those bystanders who do not.[19]

Ensuring bystander privacy and requiring reasonable notice and consent (albeit presumed consent) are crucial challenges at this time for three main reasons. First is the issue of attaining third-party consent. This problem is not new: taking pictures of people without their knowledge or consent prompted Samuel Warren and Louis Brandeis's famous 1890 article *The Right to Privacy*.[20] However, today's wearable AI products are becoming more discrete and, in many cases, are equipped with access to large language models ("LLMs"), meaning that many of them are meant to be always on, listening, and recording.

Second, the emerging wearable AI projects are more multidimensional than ever. As noted, the wearable AI industry is producing more than just fitness and health devices;[21] the new wave of products will be present in all aspects of life. A screenless device such as Humane's Ai Pin aims to be the product for a post-smartphone future.[22] Open AI has initiated a similar billion-dollar AI

[15] Editorial, *Google Glass Is the Creepy Innovation We Didn't Want*, CHI. TRIB. (May 23, 2019, 10:19 AM), https://www.chicagotribune.com/opinion/editorials/ct-glass-google-0121-20150120-story.html [https://perma.cc/AUG8-MWMS]; *see also* Larry Downes, *What Google Glass Reveals About Privacy Fears*, HARV. BUS. REV. (May 23, 2013), https://hbr.org/2013/05/what-google-glass-reveals-abou [https://perma.cc/3DJ3-E8BL] (describing "moral panic" based on privacy concerns about Google Glass).

[16] *Introducing the New Ray-Ban | Meta Smart Glasses*, META (Sept. 27, 2023), https://about.fb.com/news/2023/09/new-ray-ban-meta-smart-glasses [https://perma.cc/5YRF-PGH4].

[17] KASHMIR HILL, YOUR FACE BELONGS TO US: A SECRETIVE STARTUP'S QUEST TO END PRIVACY AS WE KNOW IT 249 (2023).

[18] *Id.* at 275-76 (describing agreement between Clearview AI and U.S. Air Force to develop glasses prototype).

[19] *Id.* at 276-77.

[20] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 211 (1890).

[21] For a review of privacy and health wearable AI, see I. Glenn Cohen, *Informed Consent and Medical Artificial Intelligence: What To Tell the Patient?*, 108 GEO. L.J. 1425 (2020).

[22] Tilley, *supra* note 2.

project.[23] While it may take time for these new devices to become mainstream and overcome their initial glitches,[24] these companies will only keep making their devices better.[25] And sooner than later, wearable AI's prevalence and its multifunctionality with audio and visual recording capabilities will cause pervasive privacy challenges for third-party bystanders.

Finally, the new wave of wearable AI products prompts an important question for product designers: Should the focus be on privacy or on user friendliness? This, too, is not new. A website that collects cookies awkwardly asks the user to answer questions and give consent, which slows down the interaction with the website. Yet the new wearable devices are not only aiming for the consent of their end users, but, as they interact with their surroundings and bystanders, they are also trying to introduce ways to alert nonusers of their presence.

Companies have reluctantly begun introducing privacy-enhancing features, but doubt continues to exist, and frictions appear to be as minimal as possible. For example, the creators of Rewind Pendant promise a privacy-preserving product, but struggle to concretely introduce a method to ensure third-party privacy.[26]

This Article builds on the privacy-by-design agenda[27] and argues that to ensure privacy and a responsible AI deployment, regulators should mandate bystander notice and consent. To this end, the designers of the wearable AI products must introduce privacy frictions: noticeable and tangible steps that would alert the third party exposed to the device of its presence and allow the bystander to make an informed choice. While attaining consent from every person may be difficult, the privacy friction can serve as a form of notice-and-presumed consent. For the purposes of privacy frictions, the bystander is not just anyone who is in the vicinity of the device, but the person that the

---

[23] Jess Weatherbed, *Details Emerge on Jony Ive and OpenAI's Plan To Build the 'iPhone of Artificial Intelligence'*, VERGE (Sept. 28, 2023, 5:20 AM), https://www.theverge.com/2023/9/28/23893939/jony-ive-openai-sam-altman-iphone-of-artificial-intelligence-device [https://perma.cc/C6QM-VUCD].

[24] For example, the Ai Pin has faced negative reviews after its initial release. *See, e.g.*, Marques Brownlee, *The Worst Product I've Ever Reviewed… For Now*, YOUTUBE (Apr. 14, 2024), https://www.youtube.com/watch?v=TitZV6k8zfA.

[25] *But see* Riley MacLeod, *Clap or AI Gets It: Can Bad Reviews Kill Companies? It's a Start.*, AFTERMATH (Apr. 17, 2024, 8:48 AM), https://aftermath.site/humane-ai-marques-brownlee [https://perma.cc/MNZ2-HEFE] ("[T]he sooner everyday people stop doing life support for AI's potential, the faster this can all be over."); Chris Person, *Why Would I Buy This Useless, Evil Thing: There's No Need for an AI Device*, AFTERMATH (Jan. 10, 2024, 2:03 PM) https://aftermath.site/why-would-i-buy-this-useless-evil-thing [https://perma.cc/VW3U-YY4T] (arguing that Rabbit R1 is poorly designed and should not have been made).

[26] Rewind, *How Can Rewind Prevent People from Being Recorded Without Their Consent?*, YOUTUBE (Oct. 4, 2023), https://www.youtube.com/watch?v=sZmG2tBzbCk.

[27] Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1411-12 (2011) ("[P]rivacy by design is . . . a systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture.").

device is directly interacting with, whether the bystander is aware of the interaction or not.[28] In other words, when the device is directly interacting with a bystander and engaging in collecting information about them, be it audio or visual, the device must have privacy frictions to put the bystander on notice and give them the opportunity to contest to their image or audio, and in general their likeness,[29] from being appropriated by the device.

These privacy functions will ensure a human-centered wearable AI privacy design and will also be in line with the value-sensitive design ("VSD") method. VSD emphasizes the importance of considering the impact of technology not only on the end-users, but also "communities, and society at large, and [it] seeks to align design decisions with these stakeholders' values and interests."[30] Privacy frictions help realize the VSD goal in seeking to "create technology that not only meets functional requirements but also considers the ethical implications and social consequences of technology."[31]

These privacy frictions can also ensure a safe and responsible AI device, which has been outlined as an essential part of the deployment and use of AI in the new Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[32]

The idea of incorporating privacy frictions for wearable AI as a form of notice and consent is a viable proposal that builds on prior scholarship in this area. Indeed, scholars have been considering new methods for notice and choice, and frictions have been incorporated since 2012. One author suggested "experience" in lieu of traditional notice for online users.[33] Other authors have proposed introducing frictions to slow down sharing on social media platforms.[34] Some have called for "obscurity by design," in the social

[28] *See* discussion *supra* note 12.

[29] For the argument of how data can be our personal likeness, see Zahra Takhshid, *Data as Likeness*, 112 GEO. L.J. (forthcoming 2024) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210660).

[30] Niloufar Salehi, *The Glossary of Human-Centered AI*, NILOUFAR'S SUBSTACK (May 3, 2023), https://niloufars.substack.com/p/the-glossary-of-human-centered-ai [https://perma.cc/26HX-WTKX] (citing Batya Friedman, Peter H. Kahn, Jr. & Alan Borning *Value Sensitive Design and Information Systems*, *in* EARLY ENGAGEMENT AND NEW TECHNOLOGIES: OPENING UP THE LABORATORY 55, 95 (Neelke Doorn, Daan Schuurbiers, Ibo van de Poel & Michael E. Gorman eds., 2013)).

[31] *Id.*

[32] Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

[33] M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1027 (2013).

[34] William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 63 (arguing that when someone has to push a button or use voice commands to share data they are experiencing frictions that prevent automatic sharing of data); Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 689 (2013) (discussing further frictionless sharing).

media and the internet context.[35] More recently, privacy scholars have proposed "desirable inefficiency" as an agenda in design to be further studied.[36] Scholars have also argued that "friction-in-design" regulation can pass the First Amendment hurdle and only trigger intermediate security.[37] This Article builds on these scholarly works and brings the concept of privacy frictions into the conversation regarding privacy design in the wearable AI industry.

Part I discusses the contemporary method of attaining consent with privacy notices. It illustrates the shortcomings of the traditional method when applied to wearable AI devices. Part II articulates the concept of privacy frictions and how it can promote a culture in the AI industry that values privacy.

This Article has a narrow focus: it does not address privacy concerns of AI software applications (synthetic AI) that use third-party image or voice data without *physically* interacting with the third party, such as deepfake video or audio.[38] It also does not address the use of AI devices by a governmental actor. Its sole focus is the use of wearables equipped with audio- and video-recording capabilities in the hands of citizens.

I. THE OLD PRIVACY NOTICE: I AGREE CHECKBOX

The traditional model of obtaining consent for data collection and privacy practices has been through written notices. These include the basic "I Agree" checkbox on website privacy policies, "I have read and agree to the terms and conditions" on applications on phones, and other similar phrasings that state that the user understands and agrees to the data collection practices of the product or software they are using. Privacy scholars have long contested the value and

[35] Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 385 (2013) ("[O]bscurity is the optimal protection for most online social interactions and, as such, is a natural locus for design-based privacy solutions for social technologies.").

[36] Paul Ohm & Jonathan Frankle, *Desirable Inefficiency*, 70 FLA. L. REV. 777, 777 (2019) ("Desirable inefficiency is an example of a design pattern that engineers have organically and voluntarily adopted to make space for human values.").

[37] Brett Frischmann & Susan Benesch, *Friction-in-Design Regulation as 21st Century Time, Place, and Manner Restriction*, 25 YALE J.L. & TECH. 376, 420 (2023) (arguing friction-in-design regulations on private companies should trigger intermediate scrutiny analogous to time, place, and manner regulations under First Amendment); *see also* Hard Fork, *Google's Trial Heats Up + How To Wear A.I. + It's Our Birthday!*, N.Y. TIMES at 27:11 (Oct. 6, 2023), https://www.nytimes.com/2023/10/06/podcasts/hard-fork-google-trial.html (discussing wearable AI and its frictionless design that could jeopardize privacy); Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 582 (2021) (addressing socioeconomic and normative centrality of data relations and data production's social effects).

[38] I have addressed this issue in another piece where I argue personally identifiable data should be considered as likeness, which is covered by privacy torts. Takhshid, *supra* note 29 (manuscript at 56). Once our image and voice, in addition to other personal data, is enlisted as personal likeness and our digital persona, we then gain the right to sue in court for privacy breaches. *Id.*

effectiveness of such "I Agree" checkboxes for ensuring information privacy.[39] Some of the problems of this approach include consumers not reading these notices,[40] difficulty in understanding them,[41] usage of vague terms,[42] lack of genuine choice due to the need to use the subject of the notice, and power imbalance of the parties.[43] The list of issues with such "choice illusion"[44] is long.

Some scholars have argued for limiting the cases in which courts uphold boilerplate contracts.[45] On the other hand, some scholars have written on the benefits of boilerplate contracts in a fast-moving society.[46] A dive into these two sides is beyond the scope of this Article. In today's market, written notices that purport that the user understands and gives consent to the data collection remain the dominant method.

To optimize such practices, the American Law Institute's project on data privacy distinguishes between transparency statements and individual notice.[47] Transparency statements are statements aimed at regulators that allow for accountability and assessment of the entity's data-collection practices with an eye towards informing the public about the entity's policies and practices.[48] Individual notice, however, is "intended to provide information to the individual whose personal data is used."[49]

---

[39] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1685 (1999) ("Self-reliant consent cannot fulfill its assigned role if individuals are guided into making uninformed, nonvoluntary exchanges.").

[40] *See id.* (discussing how individuals may not bother to read an informed consent screen).

[41] Researchers have found that simplifying the language of privacy policies barely improved consumer comprehension, stating "even the most readable policies are too difficult for most people to understand and even the best policies are confusing." Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L.J. 61, 80 (2014) (quoting Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley & Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats*, *in* PRIVACY ENHANCING TECHNOLOGIES 37, 52 (Ian Goldberg & Mikhail J. Atallah eds., 2009)).

[42] *See id.* at 73.

[43] Schwartz, *supra* note 39, at 1612-15.

[44] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 462 (2016).

[45] *See, e.g.*, MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 131-33 (2013); Zahra Takhshid, *Assumption of Risk in Consumer Contracts and the Distraction of Unconscionability*, 42 CARDOZO L. REV. 2183, 2197-03 (2021); Andrew Tutt, *On the Invalidation of Terms in Contracts of Adhesion*, 30 YALE J. ON REGUL. 439, 441 (2013); Justin P. Green, *The Consumer-Redistributive Stance: A Perspective on Restoring Balance to Transactions Involving Consumer Standard-Form Contracts*, 46 AKRON L. REV. 551, 597-98 (2013).

[46] Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 385 (2014) (noting benefits include "increased economic efficiency, improved security, better personalization of services, increased availability of relevant information, and innovative platforms for communication").

[47] PRINCIPLES OF THE L., DATA PRIV. § 3 (AM. L. INST. 2020).

[48] *Id.* § 3 cmt.a.

[49] *Id.*

The Data Privacy Principles differentiate between two types of notices: general notice and heightened notice. Heightened notice is required for circumstances in which "policies and practices are unexpected or when they pose a significant risk of material harm to some individuals."[50] The criterium for unexpectedness is the reasonable person and their expectation of consistency of the practice with other data controllers.[51]

One example of significant risk is the collection of information about health conditions.[52] Collecting health information is the function of many, if not the majority of, wearable AI devices such as Fitbit, Apple Watch, Whoop, and smart rings.[53] "Wearables are usually worn or incorporated into the body, thus providing sensory and scanning features that facilitate biofeedback and tracking."[54] "Because sensors have become inexpensive, manufacturers are including them in increasingly more products, such as smart socks, sports bras, smart bikinis, smart suits (by Samsung), smart glasses, yoga pants, and so on."[55] For example, Oura is a smart ring that collects "body responses during sleep and daily activity."[56] In such a climate, the requirement for transparent statements and privacy notices are crucial for the wearable AI industry, as data breaches in this sector have also occurred. In one incident "over 61 million fitness tracker records from Apple and Fitbit were exposed online, compromising the data privacy of their users."[57]

---

[50] *Id.* § 4 cmt.d.

[51] *Id.*

[52] *Id.* For an analysis of informed consent in the medical AI industry, see generally Cohen, *supra* note 21.

[53] *What Whoop Measures*, WHOOP, https://www.whoop.com/us/en/the-data/ (last visited May 14, 2024) ("WHOOP is [a] wearable that tracks . . . scientifically significant biometric data points and then coaches you on ways to make the changes to unlock your best."); OURA RING, https://ouraring.com [https://perma.cc/89SF-YMKC] (last visited May 14, 2024) (noting Oura Ring is a wearable device that captures over twenty biometric readings such as heart rate, body temperature, and blood oxygen).

[54] Phaik Lin Goh, *supra* note 11, at 30 (citing Kiana Tehrani & Andrew Michael, *Wearable Technology and Wearable Devices: Everything You Need To Know*, WEARABLE DEVICES MAG. (Mar. 26, 2014), https://web.archive.org/web/20140413030758/http://www.wearabledevices.com/what-is-a-wearable-device).

[55] Gutierrez, *supra* note 11, at 26 (citing Michael Sawh, *The Best Smart Clothing: From Biometric Shirts to Contactless Payment Jackets*, WAREABLE (Apr. 16, 2018), https://www.wareable.com/smart-clothing/best-smart-clothing [https://perma.cc/E3ZE-YQRH]).

[56] *Oura Teams Privacy Policy*, OURA RING, https://cloud.ouraring.com/legal/teams/privacy-policy [https://perma.cc/E9P6-JZXR] (last updated Apr. 15, 2020).

[57] Anna Sui, Wuyou Sui, Sam Liu & Ryan Rhodes, *Ethical Considerations for the Use of Consumer Wearables in Health Research*, DIGIT. HEALTH 1, 2 (Feb. 1, 2023); *see also* Jason Peres da Silva, *Privacy Data Ethics of Wearable Health Technology*, WARREN ALPERT MED. SCH. (May 4, 2023), https://digitalhealth.med.brown.edu/news/2023-05-04/ethics-wearables [https://perma.cc/Q3TS-LJ7P] ("Fitbit, a popular fitness tracking device, faced a class-action lawsuit in 2011 for allegedly selling personal health data to third-party advertisers without user consent.").

But these privacy notices and transparency statements for obtaining consent in the wearable AI industry are not as beneficial as they are—to whatever degree that is—for software products. This stems from the separation of the product and the privacy notice. For wearable AI products, the privacy notices and transparency statements are typically outlined in different ways, such as an application on the user's phone or on the website of the product.[58] Many wearable AIs are screenless, and users are unable to access a privacy policy through the devices themselves.[59] This separation could potentially create a mental gap between the product's main function and its constant data collection.

Such a mental gap could also impact the consumer's expectation of privacy. The reasonable person that uses a wearable AI could have a different mental model of the privacy protection the device offers than the reasonable person who checks the "I Agree" box for a software application on their cellphone. Therefore, the reasonable person standard for a consumer of wearable AI should be modified to include the inherent characteristics of the wearable AI products that differentiate them from software.

Taking expectations into consideration in lieu of or in addition to the traditional notice could provide a more realistic form of consent to data collection practices of wearable AI devices. Privacy scholars have identified the increasing prevalence of incorporating expectations into what entails deception for Federal Trade Commission ("FTC") privacy enforcement actions.[60] Such expectations should be measured "from the transaction as a whole and not just from what is buried and often unread in privacy policy."[61] Regulators could differentiate between software privacy policies and wearable AI privacy notices.

In any event, such notices and transparency statements are all targeted at the consumer, not the third party (i.e., the bystander). The manufacturer of a wearable AI device does not create an obligation or a commitment to privacy protection for third parties, despite general statements of such nature.[62]

II. THE NEW PRIVACY NOTICE FOR BYSTANDERS: FRICTIONS

The emergence of ChatGPT and access to LLMs has enabled many wearable AI companies to work toward a "post-smartphone" era in which

[58] *E.g.*, *Oura Teams Privacy Policy*, *supra* note 56.

[59] Phaik Lin Goh, *supra* note 11, at 31.

[60] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 667 (2014); *see also* Calo, *supra* note 33, at 1061 ("There are many examples of the FTC bringing enforcement proceedings and using the company's privacy notices as evidence that the company violated user expectations—indeed, the bulk of the agency's enforcement activity follows this route.").

[61] NEIL RICHARDS, WHY PRIVACY MATTERS 192 (1st ed. 2021).

[62] *See, e.g.*, *Designed for Privacy, Controlled by You.*, META, https://about.meta.com/ray-ban-stories-privacy/ [https://perma.cc/5W5H-NGJ9] (last visited May 14, 2024) ("Built for your privacy and others' too. The capture LED light lets people know when you're using the camera to capture content or going live. If the LED is covered, you will not be able to start recording, and you'll be notified to clear it.").

wearables function as personal assistants, signifying an "inflection point"[63] with wearable AI technology. "In 2022, the global wearable AI market size was valued at USD 21.2 billion and is expected to grow at a [rate] of 29.8% from 2023 to 2030."[64] Indeed, "[t]he scale and pace of society's digital transformation suggest that what is unfolding are not just gradual technological changes, but rather seismic shifts in the information ecosystem that call for a deeper rethinking of privacy."[65] With a shift in AI wearables market and consumers, we must consider bystander privacy and the need for a robust notice and consent mechanism, which has been overlooked.[66]

With the advent of Clearview AI, facial recognition technology became an early example of advanced AI where the bystander's privacy was put into serious question.[67] Responses to this technology have varied. There are those who have written on the positive aspects of the technology.[68] On the other hand, there are privacy advocates who argue that even limited use, such as in the hands of law enforcement, is dangerous.[69] This group even advocates for

[63] Urs Gasser, *Futuring Digital Privacy: Reimaging the Law/Tech Interplay*, *in* BIG DATA AND GLOBAL TRADE LAW 195, 197 (Mira Burri ed., 2021).

[64] Oleksandra Furman & Anton Baryshevskiy, *How AI Wearable Technology in Healthcare Helps Serve Patients Better*, MIND STUDIOS (Sept. 20, 2023), https://themindstudios.com/blog/ai-and-wearable-technology-in-healthcare/ [https://perma.cc/79TK-NCX8].

[65] Gasser, *supra* note 63, at 197.

[66] Alfredo J. Perez & Sherali Zeadally, *Privacy Issues and Solutions for Consumer Wearables*, IT PRO., July-Aug. 2017, at 46, 52 (noting main focus has been on wearer's privacy, not bystander's).

[67] *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html ("[Users] take a picture of a person, upload it and get to see public photos of that person, along with links to where those photos appeared.").

[68] *E.g.*, Vera Bergengruen, *Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company*, TIME (Nov. 14, 2023, 1:06 PM), https://time.com/6334176/ukraine-clearview-ai-russia/ ("Ukrainian officials have used Clearview to detect infiltrators at checkpoints, process citizens who lost their IDs, identify and prosecute members of pro-Russia militias and Ukrainian collaborators, and even to locate more than 190 abducted Ukrainian children who were transported across the border to live with Russian families."); *see also* Kirill Levashov, Note, *The Rise of a New Type of Surveillance for Which the Law Wasn't Ready*, 15 COLUM. SCI. & TECH. L. REV. 164, 170-71 (2013) (listing some ways in which facial recognition is used by law enforcement and for security purposes, such as maintaining and comparing faceprint databases with security footage, but also acknowledging serious privacy concerns).

[69] Rashmi Dyal-Chan, *Autocorrecting for Whiteness*, 101 B.U. L. REV. 191, 218 (2021) (citing Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/@hartzog/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66).

a total ban on the technology.[70] In the United States there is also no uniform regulatory approach, as states' mandates vary.[71]

One response to the challenge of bystander privacy, including in the case of facial recognition technology used in wearables, is shifting the moral, if not legal, responsibility to the third parties themselves.[72] A society could take the dominance of wearable AI as a given and ask for "an ethical mandate to protect one's own privacy."[73] In such a society, we may increasingly see privacy-enhancing technologies, products, and creative self-obfuscation methods to fight back against the privacy-endangering technologies. Examples include "glasses that hide facial features using near-infrared light"[74] or "futuristic makeover[s] involving funky checkerboard makeup and asymmetric hairstyles that [cover] key parts of the face."[75] These measures, however, are temporary in a fast-moving tech climate where companies could soon find ways to overcome them.[76]

Several AI companies have incorporated ethical responsibility language to address the third-party privacy challenge, shifting the burden of responsible use onto the consumer. For example, the website for Meta's smart glasses outlines several principles for "[h]ow to wear your smart glasses responsibly."[77] First, it notes that you should "[r]espect people's preferences" since "[n]ot everyone loves being photographed."[78] It further notes that the consumer should "be particularly mindful of others before going live."[79] Another principle is encouraging the consumer to "[t]urn off your glasses in sensitive spaces like the doctor's office, locker room, public bathroom, school or place of worship."[80] Next is the general principle of obeying the law. It also notes that the consumer

[70] *Id.* Several U.S. cities have implemented bans on the use of facial recognition technology by government agencies, including San Francisco, California and Portland, Oregon. Melanie A. Bigos, *Let's "Face" It: Facial Recognition Technology, Police Surveillance, and the Constitution*, 22 J. HIGH TECH. L. 52, 79-80 (2021).

[71] *See* Bigos, *supra* note 70, at 78 (noting all attempts to federally regulate use of facial recognition technology have failed, leaving regulatory authority to state and local governments).

[72] The use of facial recognition technology by authorities and the response to it is not the subject of this Article.

[73] Anita L. Allen, *An Ethical Duty To Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845, 846 (2013).

[74] Alfredo J. Perez, Sherali Zeadally, Luis Y. Matos Garcia, Jaouad A. Mouloud & Scott Griffith, *FacePET: Enhancing Bystanders' Facial Privacy with Smart Wearables/Internet of Things*, ELECTRONICS, Dec. 2018, at 1, 4 (footnotes omitted); *see also* HILL, *supra* note 17, at 241.

[75] HILL, *supra* note 17, at 266-67.

[76] *Id.*

[77] *Designed for Privacy, Controlled by You*, *supra* note 62.

[78] *Id.*

[79] *Id.*

[80] *Id.*

should "[u]se a voice command or clear gesture to let [others] know [they're] about to capture, particularly before going Live on [their] glasses."[81]

The responsibility language is well-intentioned, but its effectiveness in ensuring bystander privacy is questionable. Banning the use of such wearable technologies in certain spaces also seems difficult to implement. If a society values privacy, we must mandate design that incorporates this value. The idea that "there are no bad technologies, only bad users,"[82] is misguided. This is one of the reasons why privacy by design has gained popularity over the years.[83] The field of VSD is also promoting this approach, where societal values are incorporated at early stages in the design process.

What would this mean for the wearable AI industry that thrives on efficiency and a user-friendly product? It means accepting the need to introduce "privacy frictions." Building on the privacy-by-design agenda and VSD, this Article proposes expanding the notion of the traditional privacy notice and transparency statements to include "privacy frictions"—tangible steps that are noticeable by a reasonable bystander inadvertently subjected to a wearable AI device. Mandating privacy frictions for wearable AI devices improves the notice and transparency statements framework that solely focuses on users' privacy to include promoting third-party privacy. It can also serve as notice and presumed consent while giving the bystander the opportunity to contest and ask not to have their picture or video, and in a broader sense their likeness, collected by the device.[84] The presumption of consent with the opportunity to contest also addresses the concern of those who argue consent in this context is impossible or merely a legal fiction.[85]

The measures would be considered privacy frictions as they work against the intuitive design of easily recording and capturing images. Such privacy frictions do not need to follow a uniform method. They will vary from one device to the other and should be based on the specificity of the AI wearable in question. But they must provide reasonable notice to bystanders reasonably exposed to the device. What that would look like in practice is yet to be seen and will differ

[81] *Id.* (noting also that consumers should alert others of built-in LED light on glasses).

[82] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2018).

[83] *See*, *e.g.*, *id.*; Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 989 (2012).

[84] For the argument advocating for personal data as likeness, see generally Takhshid, *supra* note 29.

[85] *See*, *e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) (arguing consent is legal fiction under "privacy self-management" because it doesn't provide people using technology with meaningful control over their data); Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 126 (2018) ("[P]rivacy policy design can indeed manipulate consumers into giving up their personal data.").

from one context to the other. As such, the concept of contextual privacy[86] can also aid in determining who has been reasonably exposed to the device and thus requires notice. Privacy frictions can also "operate less like a binary switch and more like a tunable dial"[87] that will change over time based on what would be reasonable bystander notice at a given time.

Adopting privacy frictions in design choices for wearable AI products does not pose an inevitable impediment. Indeed, U.S. legislators suggested a similar approach in 2009, when a bill was proposed that would require cellphone cameras to make an audible shutter sound.[88] Although that bill was not adopted, frictions exist today and have been normalized in other instances. For example, take informed consent for cookies.[89] A VSD approach in adhering to privacy and ensuring user consent led to optimizing the process of getting the user's informed consent by adding "the criterion of minimal distraction" because "undue distraction can single-handedly undermine informed consent."[90]

Modern consumer contract law is also moving toward allowing, in some cases, for notice to serve as the assent of the buyer. For example, in shrinkwrap contracts, which traditionally entail a notice on the box of the product with detailed terms out of sight and wrapped inside the product's box, the notice sometimes satisfied the assent requirement for the formation of the contract, so long as the buyer had reasonable opportunity to reject and terminate.[91] Although contract scholars have criticized this approach and noted that the consent in such cases is a legal fiction,[92] the American Law Institute's new Restatement project on Consumer Contracts has adopted this "notice and opportunity to review"

[86] *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 155 (2004) ("[C]ontextual integrity [is] compatibility with presiding norms of information appropriateness and distribution.").

[87] Ohm & Frankle, *supra* note 36, at 784.

[88] Camera Phone Predator Alert Act, H.R. 414, 111th Cong. (2009); *see also* Zahra Takhshid, *Retrievable Images on Social Media Platforms: A Call for a New Privacy Tort*, 68 BUFF. L. REV. 139, 139 (2020) (proposing new tort for taking of unwanted images).

[89] The effect and viability of informed consent is disputed, and scholars have illustrated its shortcomings. *See, e.g.*, OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 3 (2014) ("'Mandated disclosure' may be the most common and least successful regulatory technique in American law."); RICHARDS, *supra* note 61, at 190.

[90] Friedman et al., *supra* note 30, at 63. Another online example of frictions is the CAPTCHA authentication requirement. *See* Frischmann & Benesch, *supra* note 37, at 408 n.93 (arguing that while CAPTCHAs are not "overburden[ing]," for cookie consents "fatigue and frustration may be more prevalent than toleration").

[91] *See* ProCD v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996).

[92] *E.g.*, Dee Pridgen, *ALI's Restatement of the Law of Consumer Contracts: Perpetuating a Legal Fiction?*, 32 LOY. CONSUMER L. REV. 540, 543 (2020); Nancy S. Kim, *Ideology, Coercion, and the Proposed Restatement of the Law of Consumer Contracts*, 32 LOY. CONSUMER L. REV. 456, 495 (2022).

approach for shrinkwrap consumer contracts.[93] Indeed, as scholars have noted, there is no actual assent in the notice and opportunity-to-review approach:

> In a true contractual transaction between A and B to which B knowingly and actually agrees, A is not required to show that B had reasonable notice of the contract's terms and a reasonable opportunity to review them. A must only show that B knowingly and actually agreed to the terms. The obvious purpose of the notice and opportunity-to-review requirements is to bind a consumer to a contract's form terms even if the consumer did not knowingly and actually agree to those terms, by substituting the notice and opportunity-to-review requirements for a requirement of true assent.[94]

While the costs and benefits of such an approach for consumer contracts is subject to debate,[95] the approach underscores the possibility for privacy frictions to serve as notice and consent. The required notice built in the wearable AI device can similarly serve as consent of the bystander to, for example, being recorded by the AI device, unless the bystander objects. Although such notice cannot be a true consent to knowing what the AI device will do with the data of the recorded bystander in every instance, it can provide some level of privacy protection for the third-party bystander while allowing the wearable AI industry to continue to grow.

Privacy scholars have also proposed requiring frictions in other circumstances, such as online sharing.[96] In this context, a delay in posting or sharing could help prevent oversharing and ease some privacy concerns. Some social media platforms, such as Twitter (now X), also experimented with similar measures to reduce misinformation on its platform.[97] Some scholars have also advocated for the concept of "desirable inefficiency," defined as "a design pattern that engineers have organically and voluntarily adopted to make space

---

[93] RESTATEMENT L. OF CONSUMER CONTS. § 2(b) (AM. L. INST., Tentative Draft No. 2, 2022). A similar approach has been adopted for clickwrap and browsewrap consumer contracts, which is presumably balanced out by defenses such as unconscionability.

[94] Melvin Eisenberg, *The Proposed Restatement of Consumer Contracts, if Adopted, Would Drive a Dagger Through Consumers' Rights*, YALE J. ON REGUL.: NOTICE & COMMENT (Mar. 20, 2019), https://www.yalejreg.com/nc/the-proposed-restatement-of-consumer-contracts-if-adopted-would-drive-a-dagger-through-consumers-rights-by-melvin-eisenberg/ [https://perma.cc/Y594-8ES5].

[95] *See, e.g.*, Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REGUL. 45, 47-48 (2019); Benjamin C. Zipursky & Zahra Takhshid, *Consumer Protection and the Illusory Promise of the Unconscionability Defense*, 103 TEX. L. REV. (forthcoming 2024) (manuscript at 34) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4777902).

[96] McGeveran, *supra* note 34, at 17; *see also* Richards, *supra* note 34, at 724.

[97] *Twitter Introduces Prompts To Alert Users Before Tweeting*, TALKCMO (Oct. 19, 2020), https://talkcmo.com/quick-bytes/twitter-introduces-prompts-to-alert-users-before-tweeting/ [https://perma.cc/Q6AT-3T8S] ("[W]hen people are going to retweet or quote tweet a disputed chain or link, a pop up will show indicating, 'This is disputed.' This will help users to go through the information before sharing.").

for human values."[98] Their primary focus has been on the design of code and software systems.[99] Additionally, two coauthors have argued for a broader incorporation of frictions in regulation for the good of the "digital networked society," and they "propose a descriptive framework for evaluating and comparing how different frictional measures can be instrumental."[100] These works suggest an attempt to "reimagin[e] the relationship between technology and privacy law" to address privacy crises.[101]

Specifically relevant to the focus of this Article is the early work of M. Ryan Calo, which advocates for privacy frictions to serve as notice and consent for bystanders. Before the dawn of wearable AI, he explored "experience" as a form of "privacy disclosure."[102] Calo notes that "[l]anguage is not the only means to convey information. Nor is it always the most efficient." [103] He defines what he calls "visceral notice" as a notice which "differs from traditional notice in that it does not necessarily rely on describing practices in language or symbols. Rather, it leverages a consumer's very experience of a product or service to warn or inform."[104] In his work, the design of the product and consumers' familiarity and experience with previous products is meant to put the consumer on notice.[105] This warning could also be applied to the wearable AI industry. For example, a uniform look for smart glasses could serve as notice and consent for the consumer. As for the bystander, the same familiarity is supposed to put them on notice.

While the concept of experience-as-privacy disclosures strengthens this Article's proposal for privacy frictions by suggesting something beyond mere written language to serve as privacy disclosure, it departs from this Article's proposal in its focus on familiarity to serve as a warning and consent.[106] Familiarity with wearable AI, however, can differ from one person to the other, as wearable AI continues to be too expensive for many households.[107] Regulators should not allow privacy violations merely due to their frequency. This trend exists in the realm of data collection and other means of

[98] Ohm & Frankle, *supra* note 36, at 778.

[99] *Id.* at 781 ("[W]e call for a new, interdisciplinary research agenda investigating how values can be embedded into code.").

[100] Frischmann & Benesch, *supra* note 37, at 379 n.1.

[101] Gasser, *supra* note 63, at 210.

[102] Calo, *supra* note 33, at 1027.

[103] *Id.* at 1034.

[104] *Id.* at 1030.

[105] *Id.* at 1035-38.

[106] Calo also suggests that "[t]he introduction of an anthropomorphic cue or a similar design element could drive home the fact of tracking in a way that privacy policies cannot." *Id.* at 1039.

[107] For example, the new Ai Pin starts at $699 and requires a $24 monthly service fee. *See Humane Launches Ai Pin*, *supra* note 3.

surveillance, the prevalence and frequency of which makes advocating for privacy even more challenging.[108]

Today, absent regulations that address bystander privacy in the age of wearable AI, some companies have added privacy-enhancing features to their designs. For example, Meta's smart glasses have a built-in LED light that lets others know when the wearer is capturing content or going live.[109]. The consumer will not be able to use the glasses to record if the LED light is covered. Humane's Ai Pin has a similar feature called "Trust Light."[110] The light "indicates when any sensors are active, which is managed via a dedicated privacy chip. If compromised, Ai Pin will shut down and require professional service from Humane."[111]

While these measures do not create a friction in the technical sense, they do alert third parties to active recording devices in many situations. Nevertheless, "[t]he goal should not be more notice, but better notice."[112] This initiative needs improvement. For example, when recording in a circumstance where the third party cannot see the light, the light falls short of being an effective privacy-enhancing measure. It is also impractical for blind or visually impaired individuals.

Another AI wearable, Rewind, is also struggling with bystander privacy. After success with its smartphone app, the AI start-up is working on a necklace that "can record conversations and transfer the recordings to a phone. AI then transcribes and analyzes the recorded conversations."[113] In a YouTube video, Rewind's CEO offers two privacy proposals but leaves open the question of how to ensure third-party privacy.[114] Rewind's first idea is to "only store recordings of the user and anyone else who has verbally opted in. Using voice fingerprints and speaker diarization, it's possible to identify who said what."[115] If adopted, this feature could be an effective privacy friction as it creates a hurdle in using the device which the user must overcome to ensure third-party privacy and obtain consent. Nevertheless, it presents its own challenges. For example, what if the wearer is in a space where a minor is

[108] *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 75 (2015) (arguing surveillance "capitalism aims to predict and modify human behavior as a means to produce revenue and market control").

[109] *Introducing the New Ray-Ban | Meta Smart Glasses*, *supra* note 16.

[110] *Humane Launches Ai Pin*, *supra* note 3.

[111] *Id.* The device makers also note that the Pin "isn't ordinarily collecting audiovisual data about your surroundings; it only does so when asked." Billy Perrigo, *Humane Wants Its New Ai Pin To Liberate You from Your Phone Screen*, TIME (Nov. 9, 2023, 12:19 PM), https://time.com/6333416/humane-ai-pin-launch/.

[112] Richards & Hartzog, *supra* note 44, at 463 (emphasis omitted) (arguing for honesty-based disclosure regime).

[113] Tilley, *supra* note 2.

[114] Rewind, *supra* note 26.

[115] *Id.*

present? Rewind would need to either have a technology that recognizes the age of the person based on their voice or rely on the goodwill of the wearer not to record the child's voice.

The second suggestion is to "only store text summaries of what was said, not verbatim transcripts and summaries."[116] Rewind believes that this would be as if "a fantastic note taker" is helping you to take notes.[117] In this method, the device designer is not seeking the consent of a bystander because it is not collecting and storing any audio or visual data to begin with.

These are just three examples of new wearable AI devices that, while creating an exciting product, could seriously jeopardize third-party privacy. By mandating privacy frictions, we can reduce the privacy risks and create a culture of notice and consent for bystanders that goes beyond written words. While innovation is crucial for a thriving society, contrary to what many companies claim, innovation does not inherently count as a "fundamental right."[118] Moreover, "AI systems both reflect and produce social relations and understandings of the world."[119] As Kate Crawford notes:

> Terms like "data mining" and phrases like "data is the new oil" were part of a rhetorical move that shifted the notion of data away from something personal, intimate, or subject to individual ownership and control towards something more inert and nonhuman. Data began to be described as a resource to be consumed, a flow to be controlled, or an investment to be harnessed.[120]

We are in a time when we can create a different rhetoric for wearable AI and its privacy concerns. Requiring bystander notice and a presumed consent through privacy frictions with the ability to contest can serve as an effective means to create a culture of privacy in this booming industry. The fact that companies themselves have also been thinking of creative ways to introduce such features indicates the seriousness of the challenge and their willingness to work with regulators if such mandates exist. It is important to introduce products in a way that not only allows profit for companies, but also ensures that society is ready for the innovation.

CONCLUSION

Requiring bystander notice and consent by mandating privacy frictions for wearable AI devices with audio and video recording capabilities could be a potential nuisance for the device maker and the user. But societies and regulators must make a crucial choice: preserving privacy by requiring minor frictions

---

[116] *Id.*

[117] *Introducing Rewind Pendant*, *supra* note 6.

[118] RICHARDS, *supra* note 61, at 182.

[119] KATE CRAWFORD, ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE 8 (2021).

[120] *Id.* at 113.

while allowing the wearable AI industry to thrive, or relinquishing whatever privacy that is left at the expense of convenience. The choice is ours to make, and it is still not too late.