Yale Journal of Law & Technology
Volume 26, Issue 3

Special Issue:
Yale Information Society Project
Digital Public Sphere Series

Two AI Truths and a Lie

Woodrow Hartzog[*]

Industry will take everything it can in developing artificial intelligence (AI) systems. We will get used to it. This will be done for our benefit. Two of these things are true and one of them is a lie. It is critical that lawmakers identify them correctly. In this Essay, I argue that no matter how AI systems develop, if lawmakers do not address the dynamics of dangerous extraction, harmful normalization, and adversarial self-dealing, then AI systems will likely be used to do more harm than good.

Given these inevitabilities, lawmakers will need to change their usual approach to regulating technology. Procedural approaches requiring transparency and consent will not be enough. Merely regulating use of data ignores how information collection and the affordances of tools bestow and exercise power. A better approach involves duties, design rules, defaults, and data dead ends. This layered approach will more squarely address dangerous extraction, harmful normalization, and adversarial self-dealing to better ensure that AI deployments advance the public good.

---

[*] Professor of Law and Class of 1960 Scholar, Boston University School of Law. The author wishes to thank Ryan Calo, Stacey Dogan, Evan Selinger, and Jessica Silbey for their helpful comments, Philipa Yu and Janelle Robins for their excellent research assistance, and Elisabeth Paar, Gilad Abiri, and the editors of the *Yale Journal of Law & Technology* for their excellent edits and feedback.

Essay Contents

Introduction

It's hard to know what to believe about our likely future with artificial intelligence (AI). The techno-optimists tell us that AI will be a "force for good" as it becomes integrated into almost every aspect of our lives.[1] For some, we simply need to set up guardrails so society can benefit from these systems while minimizing their harms.[2] The techno-doomers, a dramatic division of the AI hype machine, warn us that AI systems could become intelligent and powerful enough to wipe out humanity,[3] though that doesn't seem to stop them from building AI systems as fast as they can. Meanwhile, the more skeptical and even cautiously optimistic crowds are not worried about AI systems becoming so smart that they take over the world, but instead are worried that they are too dumb and that they have already taken over.[4] Societal well-being hangs in the

---

[1] Chris Vallance, *More Than 1,300 Experts Call AI a Force for Good*, BBC (July 18, 2023), https://www.bbc.com/news/technology-66218709 [https://perma.cc/W86E-LRYL]; Gideon Rosenblatt & Abhishek Gupta, *Artificial Intelligence as a Force for Good*, STAN. SOC. INNOVATION REV. (June 11, 2018), https://ssir.org/articles/entry/artificial_intelligence_as_a_force_for_good [https://perma.cc/ZWD3-3R84]; Marc Andreessen, *The Techno-Optimist Manifesto*, ANDREESSEN HOROWITZ (Oct. 16, 2023), https://a16z.com/the-techno-optimist-manifesto [https://perma.cc/TFH6-SQ88]; Mariarosaria Taddeo & Luciano Floridi, *How AI Can Be a Force for Good*, 361 SCIENCE 751 (2018).

[2] *See, e.g.*, ORLY LOBEL, THE EQUALITY MACHINE: HARNESSING DIGITAL TECHNOLOGY FOR A BRIGHTER, MORE INCLUSIVE FUTURE (2022); Orly Lobel, *The Law of AI for Good*, 75 FLA. L. REV. 1073, 1083 (2023).

[3] Kevin Roose, *A.I. Poses 'Risk of Extinction,' Industry Leaders Warn*, N.Y. TIMES (May 30, 2023), https://www.nytimes.com/2023/05/30/technology/ai-threat-warning.html [https://perma.cc/Q4MP-6P2S].

[4] *See, e.g.*, Pedro Domingos, *How to Train Your AI*, MEDIUM (Nov. 28, 2016), https://pedromdd.medium.com/how-to-train-your-ai-f5313a889957 [https://perma.cc/9QKY-TDL5] ("Computers make a lot of bad decisions because they don't know any better, from picking the wrong stock to buy from picking the wrong date for you. People worry that computers will get too smart and take over the world, but the real problem is that they're too stupid and they've already taken over the world."). For more critical reading on AI, see KATE CRAWFORD, ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE 15 (2021), which notes

balance, as our rules and frameworks for regulating AI depend on policymakers' mental models, their predictions for the affordances of AI, and how people and organizations are likely to respond to these affordances.[5] But we already know how this will play out.

The most prominent AI tools developed for use in commercial, employment, and government surveillance contexts feel handcrafted for industry exploitation and fascist oppression. Companies are already using generative AI, biometric surveillance, predictive analytics, and automated decision-making for power and profit. No matter how AI develops, there are a few dynamics we can count on. Companies are going to seek to profit from AI and will take advantage of narratives to block rules that interfere with their business models.[6] The governments that want powerful AI tools won't stand in the way.

---

that the extractive nature of AI exploits "energy and mineral resources from the planet, cheap labor, and data" on a global scale; JOY BOULAMWINI, UNMASKING AI: MY MISSION TO PROTECT WHAT IS HUMAN IN A WORLD OF MACHINES xv (2023), which highlights the ways in which AI falls well short of the promise to "overcome human limitations" and instead further entrenches and codifies existing inequities; MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD 6 (2018), which articulates the limits of AI and how "the way people talk about technology is out of sync with that digital technology actually can do"; and MEREDITH BROUSSARD, MORE THAN A GLITCH: CONFRONTING RACE, GENDER, AND ABILITY BIAS IN TECH (2023) [hereinafter BROUSSARD, MORE THAN A GLITCH], which explains how the ways in which existing inequities and biases relating to race, gender, and ability form the starting point of today's technology, and thus, create inherently racist, sexist, and ableist technochauvinistic systems.

[5] Ryan Calo, *Privacy, Vulnerability, and Affordance*, 66 DEPAUL L. REV. 591, 601-03 (2016); WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 38 (2018); Ryan Calo, *Modeling Through*, 71 DUKE L.J. 1391, 1398 (2022); JAMES J. GIBSON, *The Theory of Affordances, in* THE ECOLOGICAL APPROACH TO VISUAL PERCEPTION 127, 127-37 (1979).

[6] *See generally* AMBA KAK & SARAH MYERS WEST, AI NOW INST., 2023 LANDSCAPE: CONFRONTING TECH POWER (2023), https://ainowinstitute.org/wp-content/uploads/2023/04/AI-Now-2023-Landscape-Report-FINAL.pdf [https://perma.cc/25WR-QQUZ]; *cf.* JULIE COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF

When I was younger, I often played the game "two truths and a lie." The idea is to offer up three statements, only two of which are true, and see if others can guess the lie. It's a fun ice breaker and a great way to get to know others. It's also a helpful way to work through what is and what is likely to be.

In this Essay, I frame the pathologies related to industry's deployment of AI systems in the form of two truths and a lie. I argue that lawmakers should shape their regulatory response to AI systems around three dangerous dynamics that will be inevitable unless lawmakers intervene.

The first truth: the primary certainty of AI is that commercial actors who design and deploy it will take everything they can from us. Companies cannot create AI without data, and the race to collect information about literally every aspect of our lives is more intense than ever. The trajectory of data collection and exploitation only runs one way: *more*.

Second truth: we will get used to it. After initial protests about new forms of data collection and exploitation, we will become accustomed to these new invasions or at least will develop a begrudging and fatalistic acceptance of them.[7] Our current rules have no backstop against total exposure.

Third: this will all be done "for our benefit." And that's the lie. AI tools might benefit us, but they will not be created *for* our collective benefit. Organizations will say the deployment of facial and emotion recognition in schools is motivated by the desire to keep students focused and edified. Employers will say that the deployment of neurotechnology in the workplace is to keep employees safe and engaged. Platforms will promise that the use of eye-tracking and spatial mapping in augmented-

---

INFORMATIONAL CAPITALISM 176 (2019) (discussing telecom companies' anti-net-neutrality narrative); ARI WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 232-33 (2021) (arguing that in the data privacy context, "[m]any companies in the information industry have perfected the art of performing accountability while exercising great power behind the scenes, clearing away the discursive, legal, and procedural obstacles to extracting our data").

[7] *See* Evan Selinger & Woodrow Hartzog, *Stop Saying Privacy Is Dead*, MEDIUM (Oct. 11, 2018), https://medium.com/@evanselinger/stop-saying-privacy-is-dead-513dda573071 [https://perma.cc/A5B6-J8F7].

reality and virtual-reality environments is to better cater to your desires. Although people will probably realize *some* benefits from these tools, companies have little interest in (and show no evidence of pursuing) societal improvement. The result? The benefits of AI systems are often pretexts for market expansion into the increasingly few spaces in our lives that are not captured, turned into data, and exploited for profit.

Regardless of how AI evolves technologically, that evolution will include data capture, normalization, and industry self-dealing. Lawmakers should act accordingly. I argue that lawmakers should embrace four approaches to regulating AI: (1) Duties, (2) Design, (3) Defaults, and (4) Dead Ends ("The 4 D's of AI Regulation"). Less sturdy and insufficient procedural strategies and spotty use limits will not be enough. Only stronger, substantive approaches can help ensure that society will be better off with AI—notwithstanding the inevitable data grabs, normalization, and self-dealing that come with it.

I. Industry Will Take Everything It Can

AI systems are gluttonous for personal information. Mountains of data are necessary to train models.[8] Companies use this fact to justify all sorts of data collection, including presumptions that human information is fair game to capture and exploit—particularly if it's publicly accessible. Julie Cohen calls this move to frame human information as a source of raw materials there for the taking for economic production as the

[8] Bureau of Competition & Office of Technology, *Generative AI Raises Competition Concerns*, FED. TRADE COMM'N: TECH. BLOG (June 29, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns [https://perma.cc/XB2Y-7QB8] ("The foundation of any generative AI model is the underlying data. Developing generative AI typically requires exceptionally large datasets, especially in the pre-training step. The data used in this step forms the foundation of the model in the chosen domain, such as language or images."); *The Size and Quality of a Data Set*, GOOGLE FOR DEVS. (July 18, 2022), https://developers.google.com/machine-learning/data-prep/construct/collect/data-size-quality [https://perma.cc/6SCZ-S9SU].

biopolitical public domain.[9] Our information-law frameworks already reflect the idea that human information is a free resource to anyone with the means and drive to exploit it. But if lawmakers continue to treat human information as a raw resource ripe for capture, they will have ended the battle for privacy and human well-being in AI systems before it has even started.

The concept of the biopolitical public domain doesn't just give a free pass to companies to extract our data, it also encourages exploitation.[10] Companies collecting data that will eventually be used in AI systems are currently out of control. For years, companies have been collecting data without a clear idea of what to do with it, expecting that it could become valuable somehow.[11] AI presents the perfect opportunity to put it all to use. An example of the inevitability of data collection is the creepy prescience of targeted ads. Many of us have had the experience of discussing a product, vacation, or film, and then seeing an ad for that exact item only moments later. This has led to the widespread idea that all our Internet of Things (IoT) devices and phones are secretly listening to our

---

[9] COHEN, *supra* note 6, at 49 ("The process of constructing a public domain begins with an act of imagination that doubles as an assertion of power. An identifiable subject matter—a part of the natural world or an artifact of human activity—is reconceived as a resource that is unowned but potentially appropriable, either as an asset in itself or as an input into profit-making activity."); Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213, 213 (2017).

[10] COHEN, *supra* note 6, at 51 ("Imagining the universe of personal data as a commons ripe for exploitation is only the beginning, however. For the idea of a public domain to fulfill its imagined destiny as a site of productive labor it must be linked to more concrete logics of extraction and appropriation. By that standard, the biopolitical public domain is a construct of extraordinary power.").

[11] *See, e.g.*, VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2014); Omer Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 259 (2013) ("The big data business model is antithetical to data minimization. It incentivizes collection of more data for longer periods of time. It is aimed precisely at those unanticipated secondary uses, the 'crown jewels' of big data.").

conversations.[12] They largely aren't, except for the IoT doorbells.[13] But the truth is even more disquieting. Companies don't need to eavesdrop on us through IoT microphones because they already know so much through their massive data mining operations.[14] A recent study by Consumer Reports showed that, in some instances, nearly 48,000 different companies provided Facebook with data about one user.[15] Most of the data collected by companies isn't essential for the service.[16] It's just a grab.[17] And AI is making industry's thirst for data even more unquenchable, as companies developing

---

[12] Eric Johnson, *Your Phone Is Not Secretly Spying on Your Conversations. It Doesn't Need to.*, VOX (July 20, 2018), https://www.vox.com/2018/7/20/17594074/phone-spying-wiretap-microphone-smartphone-northeastern-dave-choffnes-christo-wilson-kara-swisher [https://perma.cc/D6BA-J2RQ].

[13] Daniel J. Dubois et al., *When Speakers Are All Ears: Understanding When Smart Speakers Mistakenly Record Conversations*, MON(IOT)R RSCH. GRP., https://moniotrlab.khoury.northeastern.edu/publications/smart-speakers-study-pets20 [https://perma.cc/A28K-Q3M9]; Yael Grauer, *Video Doorbell Cameras Record Audio, Too*, CONSUMER REPS. (May 18, 2022), https://www.consumerreports.org/home-garden/home-security-cameras/video-doorbell-cameras-record-audio-too-a4636115889 [https://perma.cc/A8G7-FN7D].

[14] Wes Davis, *48,000 Companies Sent Facebook Data on a Single Person*, VERGE (Jan. 17, 2024), https://www.theverge.com/2024/1/17/24041897/facebook-meta-targeted-advertising-data-mining-study-privacy [https://perma.cc/TD3X-T22R].

[15] Jon Keegan, *Each Facebook User Is Monitored by Thousands of Companies*, CONSUMER REPS. (Jan. 17, 2024), https://www.consumerreports.org/electronics/privacy/each-facebook-user-is-monitored-by-thousands-of-companies-a5824207467.

[16] Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1468-69 (2020).

[17] Shankar Parameshwaran, *How Data Privacy Concerns Impact Firm Performance*, KNOWLEDGE WHARTON (Dec. 5, 2023), https://knowledge.wharton.upenn.edu/article/how-data-privacy-concerns-impact-firm-performance [https://perma.cc/3PM9-EYQS]; Rob Pegoraro, *What Part of 'Get Rid of My Data' Don't Companies Get?*, FAST CO. (Nov. 27, 2023), https://www.fastcompany.com/90987233/what-part-of-get-rid-of-my-data-dont-companies-get [https://perma.cc/7APG-P69G].

these systems scrape, purchase, or directly collect as much personal data as possible to feed their models.[18]

It's not just data that industry is after. Modern AI-driven systems have the capacity to capture our time and effort and to dictate what we see and can do.[19] Industry's mandate to maximize shareholder value ensures that no human resource—including our thoughts, our relationships, our attention, our labor, and our environment—remains unexploited.[20] Companies will go as far as the most permissive interpretation of the law (and sometimes beyond).[21]

---

[18] Will Knight, *Generative AI is Making Companies Even More Thirsty for Your Data*, WIRED (Aug. 10, 2023, 12:00 PM), https://www.wired.com/story/fast-forward-generative-ai-companies-thirsty-for-your-data [https://perma.cc/H2XC-TAG9]; Samantha Cole, *Tumblr and WordPress to Sell Users' Data to Train AI Tools*, 404 MEDIA (Feb. 27, 2024, 1:21 PM), https://www.404media.co/tumblr-and-wordpress-to-sell-users-data-to-train-ai-tools [https://perma.cc/65KH-V84H].

[19] *See generally* NITA FARAHANY, THE BATTLE FOR YOUR BRAIN: DEFENDING THE RIGHT TO THINK FREELY IN THE AGE OF NEUROTECHNOLOGY (2023); KAREN LEVY, DATA DRIVEN: TRUCKERS, TECHNOLOGY, AND THE NEW WORKPLACE SURVEILLANCE (2022); JOHANN HARI, STOLEN FOCUS: WHY YOU CAN'T PAY ATTENTION—AND HOW TO THINK DEEPLY AGAIN (2022); IFEOMA AJUNWA, THE QUANTIFIED WORKER (2023); COHEN, *supra* note 6.

[20] *See generally* CRAWFORD, *supra* note 4; COHEN, *supra* note 6; SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); Kapcyznski, *supra* note 16; Andrew F. Tuch, *A General Defense of Information*, 98 WASH. U. L. REV. 1897 (2021); Neil Richards & Woodrow Hartzog, *Against Engagement*, 104 B.U. L. REV. 1151 (2024); Elettra Bietti, *The Data-Attention Imperative* (forthcoming) (on file with authors); Aileen Nielsen, *Tech Has an Attention Problem*, U.C. BERKELEY CTR. FOR LONG-TERM CYBERSECURITY WHITE PAPER SERIES (Sept. 2021), https://ethz.ch/content/dam/ethz/special-interest/gess/law-n-economics/leb-dam/documents/CLTC_Techs_Attention_Problem.pdf [https://perma.cc/KFH2-856X]; Matteo Wong, *The Lifeblood of the AI Boom*, ATLANTIC (Mar. 6, 2024), https://www.theatlantic.com/technology/archive/2024/03/nvidia-chips-gpu-generative-ai/677664 [https://perma.cc/FT7N-5VHK].

[21] *See, e.g.*, WALDMAN, *supra* note 6, at 104-26.

Even when companies voluntarily avoid dangerous AI tools, less scrupulous actors consistently undermine them.[22] For example, Google avoided implementing facial recognition technologies into its services—fearing how dangerous the tool was—only to have Clearview AI and PimEyes barge ahead.[23] Industry, as a whole, simply doesn't have the incentive or ability to voluntarily leave money on the table for the good of society.

Industry's drive to extract everything from us is buoyed by narratives that depict AI as inevitable and technological innovation as inherently beneficial.[24] Implicit in virtually every

---

[22] Chinmayi Sharma, *Setting a Higher Bar: Professionalizing AI Engineering*, LAWFARE (Dec. 12, 2023, 12:00 PM), https://www.lawfaremedia.org/article/setting-a-higher-bar-professionalizing-ai-engineering [https://perma.cc/F4ZB-GHBV] ("When safety means forgoing a competitive advantage, companies are not likely to adopt the Anthropic model of cautious research. In other words, safety is probably going to be sacrificed at the altar of commercialization."). This is a classic "race to the bottom" dynamic. *See, e.g.*, Dan Milmo, *AI-Focused Tech Firms Locked in 'Race to the Bottom', Warns MIT Professor*, GUARDIAN (Sept. 21, 2023), https://www.theguardian.com/technology/2023/sep/21/ai-focused-tech-firms-locked-race-bottom-warns-mit-professor-max-tegmark [https://perma.cc/3QYT-JU8H]; David Evan Harris, *The Race to the Bottom on AI Safety Must Stop*, CTR. FOR INT'L GOVERNANCE INNOVATION (June 16, 2023), https://www.cigionline.org/articles/the-race-to-the-bottom-on-ai-safety-must-stop [https://perma.cc/M2JH-YBZA].

[23] Kasmir Hill, *The Technology Facebook and Google Didn't Dare Release*, N.Y. TIMES (Sept. 11, 2023), https://www.nytimes.com/2023/09/09/technology/google-facebook-facial-recognition.html [https://perma.cc/UQY3-3FP9] ("While Meta's augmented reality glasses are still in development, the company shut down the facial recognition system deployed on Facebook to tag friends in photos and deleted the more than one billion face prints it had created of its users. It would be easy enough to turn such a system back on. When I asked a Meta spokesman about . . . whether the company might put facial recognition into its augmented reality glasses one day, he would not rule out the possibility.").

[24] Josh Taylor, *Rise of Artificial Intelligence Is Inevitable but Should not Be Feared, 'Father of AI' Says*, GUARDIAN (May 6, 2023, 8:00 PM), https://www.theguardian.com/technology/2023/may/07/rise-of-artificial-intelligence-is-inevitable-but-should-not-be-feared-father-of-ai-says [https://perma.cc/25CQ-MN42]; CGI Energy Transition Talks, *Generative*

industry proposal for "trustworthy AI" and "ethical AI principles" is the idea that it would be a bad thing to impede the progress of AI.[25] People that adhere to the "effective accelerationist" ideology argue that "artificial intelligence and other emerging technologies should be allowed to move as fast as possible, with no guardrails or gatekeepers standing in the way of innovation."[26] The implication of this argument is that humans should submit to industry when they come to harvest our lives for more efficient and accurate models.

The data, labor, and attention imperatives created by the drive for profit and power highlight the sad reality of our exposure: without appropriate legal intervention, surveillance and exploitation of human behavior only increases. As I wrote in an article with Evan Selinger and Johanna Gunawan: "The trajectory of surveillance has never deviated from increased exposure. Today, more sensors are used to watch more people for more purposes and longer durations than ever before."[27]

This inevitability manifests in subtle but persistent expansions of affordances and deployments until it completely colonizes whole parts of our lives.[28] Brett Frischmann and Evan

---

AI Is Inevitable but a Structured, Responsible Approach Is Critical, CGI (Jan. 9, 2024), https://www.cgi.com/en/podcast/energy-utilities/generative-artificial-intelligence-inevitable-responsible-approach-critical [https://perma.cc/LX85-95RB]; Andreessen, *supra* note 1 ("Technological innovation in a market system is inherently philanthropic, by a 50:1 ratio. Who gets more value from a new technology, the single company that makes it, or the millions or billions of people who use it to improve their lives?").

[25] Jessica Fjeld et al., *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y (2020); *Responsible AI,* META, https://ai.meta.com/responsible-ai [https://perma.cc/2HKM-MPS5].

[26] Kevin Roose, *This A.I. Subculture's Motto: Go, Go, Go*, N.Y. TIMES (Dec. 10, 2023), https://www.nytimes.com/2023/12/10/technology/ai-acceleration.html [https://perma.cc/75FN-MVND] ("Effective Accelerationism (often shortened to 'e/acc,' pronounced 'e-ack') is a loosely organized movement devoted to the no-holds-barred pursuit of technological progress.").

[27] Woodrow Hartzog, Evan Selinger & Johanna Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, 101 WASH. U. L. REV. 717, 720 (2024).

[28] *See generally* Woodrow Hartzog & Evan Selinger, *The Internet of Heirlooms and Disposable Things*, 17 N.C. J.L. & Tech. 581 (2016).

Selinger have called this "techno-social engineering creep," and once you learn to recognize it, you see it everywhere.[29] IoT doorbells were first designed to provide a simple video feed of the area right in front of the door. Now, they are being outfitted with AI-powered facial recognition and anomaly-recognition technologies and have a range of 1.5 miles.[30] It would take only a small percentage of people to adopt these tools to ensure that there would be nowhere in public anyone could remain obscure.[31] Likewise, "smart" watches and earbuds were first designed just to detect when you'd like to use them. Maybe they could do something simple, such as measure your pulse. Now, companies offer to monitor your mood and sleep habits; from that foothold, they plan to move to neurotechnology to

---

[29] BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 35-42 (2018).

[30] Amrita Khalid, *This Security Camera's 1.5-Mile Range Is Perfect for Your Sprawling Mansion*, VERGE (Jan. 8, 2024, 3:05 PM), https://www.theverge.com/2024/1/8/24030379/abode-edge-camera-long-range-facial-recognition-ai-ces-2024 [https://perma.cc/ZJ8F-YBUU].

[31] Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1345-46 (2015) [hereinafter Hartzog & Selinger, *Loss of Obscurity*] ("[W]e argue that the concept of 'obscurity,' which deals with the transaction costs involved in finding or understanding information, is the key to understanding and uniting modern debates about government surveillance."); Woodrow Hartzog & Evan Selinger, *Increasing the Transaction Costs of Harassment*, 95 B.U. L. REV. ANNEX 47, 49-50 (2015) [hereinafter Hartzog & Selinger, *Costs of Harassment*]; Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* SPACES FOR THE FUTURE: A COMPANION TO PHILOSOPHY OF TECHNOLOGY 119, 122 (Joseph Pitt & Ashley Shew eds., 2018); *see also* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 5 (2013) ("We argue the case for obscurity for two reasons. First, we argue that obscurity is a common and natural condition of interaction, and therefore human expectation of obscurity will transfer to the domains in which we spend time, both physical and virtual. Second, we argue that obscurity is a desirable state because we are protected by an observer's inability to comprehend our actions, and therefore social practice encourages us to seek obscurity."); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 388 (2013); Mark P. McKenna & Woodrow Hartzog, Taking Scale Seriously in Robotics and A.I. Law 20-21 (Sept. 18, 2023) (unpublished manuscript) (available at: https://www.bu.edu/law/files/2023/09/McKenna-Hartzog-Scale-v7.pdf [https://perma.cc/D94T-8D4P]).

monitor your thoughts.[32] Where companies once tracked people's clicks and texts, they now collect data on sound, space, eye movement, heartbeat, brain activity, and more.[33]

In pursuit of AI market expansion, companies will invade every aspect of our lives. AI tools are already being deployed to "optimize" our places of work. Employers use dubious affect recognition to screen out prospective employees who don't have the right facial expressions.[34] Once people are hired, companies increasingly deploy AI to micromanage as many aspects of our work as the technology will allow, including how long we take bathroom breaks and whether our attention is completely focused on our task.[35] No daydreaming, relaxing, or

---

[32] Apple Inc., Application No. 18/094,841 (filed Jan. 9, 2023); FARAHANY, *supra* note 19, at 21-23; Anugraha Sundaravelu, *Apple's $3,499 Vision Pro Headset Could 'Read Your Mind'*, METROUK (June 8, 2023, 10:53 AM), https://metro.co.uk/2023/06/07/apples-3499-vision-pro-headset-could-read-your-mind-18910898 [https://perma.cc/APA6-LJZD]; Luke Hurst, *These 'Neurohacking' Headphones Use AI to Track Your Brain Signals to Help You Stay Productive*, EURONEWS (June 16, 2023, 9:51 PM), https://www.euronews.com/next/2023/06/14/these-neurohacking-headphones-use-ai-to-track-your-brain-signals-to-help-you-stay-producti [https://perma.cc/77B4-RUJ2].

[33] Jasmine E. McNealy, *Sonic Privacy*, 24 YALE J.L. & TECH. 365 (2022); JOSEPH TUROW, THE VOICE CATCHERS: HOW MARKETERS LISTEN IN TO EXPLOIT YOUR FEELINGS, YOUR PRIVACY, AND YOUR WALLET 1-33 (2021); FARAHANY, *supra* note 19, Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 VAND. J. ENT. & TECH. L. 1, 30 (2020); Joseph Jerome, *Pretty Soon, Your VR Headset Will Know Exactly What Your Bedroom Looks Like*, WIRED (Oct. 3, 2023, 8:00 AM), https://www.wired.com/story/virtual-reality-meta-wearables-privacy [https://perma.cc/D68H-LNAW]; Kyle Orland, *Meta Will Start Collecting "Anonymized" Data about Quest Headset Usage*, ARS TECHNICA, https://arstechnica.com/gaming/2024/02/meta-will-start-collecting-anonymized-data-about-quest-headset-usage [https://perma.cc/J38C-ZU2C].

[34] Anna Kramer, *The (Possibly Dystopian) Rise of the Automated Video Interview*, PROTOCOL (May 27, 2022), https://www.protocol.com/workplace/automated-video-interviews-hirevue-modernhire [https://perma.cc/55CB-VG54].

[35] Leonie Cater & Melissa Heikkilä, *Your Boss Is Watching: How AI-Powered Surveillance Rules the Workplace*, POLITICO (May 27, 2021, 11:00 AM), https://www.politico.eu/article/ai-workplace-surveillance-facial-

personal time allowed. AI is being pitched to schools for the same kind of optimization.[36] As if students didn't have enough to worry about, now "[m]ultiple cameras spread throughout the room will take attendance, monitor whether students are paying attention and detect their emotional states, including whether they are bored, distracted or confused.[37] Faculty won't be spared either. AI provides a turnkey tool to retaliate against scholars and teachers who step out of line even a little.[38] In short, organizations will deploy AI as a micromanaging misery machine.

Our social lives will also be affected, as AI companies hawk tools to automatically take attendance at church, correct your tone when you're texting others, and write thank-you notes

---

recognition-software-gdpr-privacy [https://perma.cc/E2B4-MW2G]. *See generally* AJUNWA, *supra* note 19; Susan, D'Agostino, *Facial Recognition Heads to Class. Will Students Benefit?*, INSIDE HIGHER ED (Feb. 27, 2024), https://www.insidehighered.com/news/tech-innovation/teaching-learning/2024/02/27/facial-recognition-heads-class-will-students [https://perma.cc/4XU9-6ED9].

[36] Amar Toor, *This French School Is Using Facial Recognition to Find Out When Students Aren't Paying Attention*, VERGE (May 26, 2017, 3:28 AM), https://www.theverge.com/2017/5/26/15679806/ai-education-facial-recognition-nestor-france [https://perma.cc/5Z2K-SNZK]; Karen Hao, *China has Started a Grand Experiment in AI Education. It Could Reshape How the World Learns.*, MIT TECH. REV. (Aug. 2, 2019), https://www.technologyreview.com/2019/08/02/131198/china-squirrel-has-started-a-grand-experiment-in-ai-education-it-could-reshape-how-the [https://perma.cc/2QU4-GD64] ("Algorithms measure how much time the students spoke English in class, the accuracy of their English pronunciation, and basic indicators of their engagement and joy, such as the number of times they opened their mouth to speak and laugh. Earlier this year, the company created several physical classrooms equipped with cameras and microphones to produce similar analyses.").

[37] D'Agostino, *supra* note 35.

[38] *See* Carrie Spector, *Feedback from an AI-Driven Tool Improves Teaching, Stanford-Led Research Finds*, STAN. GRADUATE SCH. EDUC.: RSCH. STORIES (May 8, 2023), https://ed.stanford.edu/news/feedback-ai-driven-tool-improves-teaching-stanford-led-research-finds [https://perma.cc/CN5P-3A3K]; Ian Bogost, *The Plagiarism War Has Begun*, ATLANTIC (Jan. 4, 2024), https://www.theatlantic.com/technology/archive/2024/01/plagiarism-war-claudine-gay/677020 [https://perma.cc/HP2V-UVPX].

when you can't be bothered.[39] Companies have even made facial recognition and profiling part of buying a candy bar through a vending machine.[40] Not even the humble shopping cart is safe as companies such as Instacart plan on installing screens on carts to show ads that are personalized to your shopping behavior.[41] Law enforcement has also begun to employ AI, using ChatGPT to fill out police reports.[42] The Pentagon is eager to incorporate generative AI into its processes for summarizing information, war-gaming, and real-time decision-making.[43] Companies are even trying to change our physical infrastructure for walking and driving to accommodate AI tools like delivery robots.[44]

AI will also poison our information ecosystem as companies deploy generative tools to scam at scale.

---

[39] *See* JIBBLE, https://www.jibble.io/church-attendance [https://perma.cc/3BBV-8S67]; *Tone Checker*, SAPLING, https://sapling.ai/utilities/tonehttps://sapling.ai/utilities/tone [https://perma.cc/4FCY-C4JC]; Matt Ellis, *How to Use AI to Write a Thoughtful Thank-You Note*, GRAMMARLY (Aug. 10, 2023), https://www.grammarly.com/blog/ai-thank-you-note [https://perma.cc/8KML-HQAG].

[40] Ashley Belanger, *Vending Machine Error Reveals Secret Face Image Database of College Students*, ARS TECHNICA (Feb. 23, 2024, 5:02 PM), https://arstechnica.com/tech-policy/2024/02/vending-machine-error-reveals-secret-face-image-database-of-college-students [https://perma.cc/5YZY-8GFX]

[41] Alex Bitter, *Smart Shopping Carts with Customized Ads Are the Future of Grocery Shopping, According to Instacart*, BUS. INSIDER (Jan. 8, 2024, 3:27 PM), https://www.businessinsider.com/instacart-smart-shopping-carts-with-tailored-ads-are-coming-2024-1 [https://perma.cc/LKW5-WD9B].

[42] Jason Potts, *The Impact of Large Language Models on Police Report Writing and Beyond*, POLICE1 (Feb. 12, 2024, 9:57 AM), https://www.police1.com/tech-pulse/the-impact-of-large-language-models-on-police-report-writing-and-beyond [https://perma.cc/EK3D-WQAH].

[43] Eva Dou et al., *Pentagon Explores Military Uses of Large Language Models*, WASH. POST (Feb. 20, 2024), https://www.washingtonpost.com/technology/2024/02/20/pentagon-ai-llm-conference [https://perma.cc/W5HV-GUCQ].

[44] Jason Koebler, *'Student Should Have a Healthy-Looking BMI': How Universities Bend Over Backwards to Accommodate Food Delivery Robots*, 404 MEDIA (Jan. 17, 2024, 10:52 AM), https://www.404media.co/student-should-have-a-healthy-looking-bmi-how-universities-bend-over-backwards-to-accommodate-starship-food-delivery-robots [https://perma.cc/4F7R-D47Q].

Phenomena like AI obituary spam are just the beginning of the flood of false information that's cheap and easy to produce.[45] What's worse is that new AI models will then scrape, learn from, and be built on top of this information pollution, creating a cycle in which a model built on misinformation and fraud keeps eating itself. An ouroboros of crap.[46]

The backslide of democracy and the rise of authoritarian governments around the world will only amplify these problems. Facial recognition is the perfect tool of oppression.[47] Governments are only a subpoena or warrant away from the data collected by AI-powered doorbells, AR/VR devices, chatbots, and neurotechnology headphones. Furthermore, the discourse and pressure to collect and use everything for AI are supercharged by the misguided narrative that if we restrict the development and use of AI, we'll fall behind in the "AI arms race" with other countries.[48] Governments are one of the main

---

[45] Karl Bode, *False AI Obituary Spam the Latest Symptom of Our Obsession with Mindless Automated Infotainment Engagement*, TECHDIRT (Feb. 20, 2024), https://www.techdirt.com/2024/02/20/false-ai-obituary-spam-the-latest-symptom-of-our-obsession-with-mindless-automated-infotainment-engagement [https://perma.cc/K7YU-JSRP]; Emanuel Maiberg, *Ghost Kitchens Are Advertising AI-Generated Food on DoorDash and Grubhub*, 404 MEDIA (Feb. 27, 2024, 9:07 AM), https://www.404media.co/ghost-kitchens-are-advertising-ai-generated-food-on-doordash-and-grubhub [https://perma.cc/GRA9-GBW2].

[46] James Vincent, *AI Is Killing the Old Web, and the New Web Struggles to Be Born*, VERGE (June 26, 2023, 11:25 AM), https://www.theverge.com/2023/6/26/23773914/ai-large-language-models-data-scraping-generation-remaking-web [https://perma.cc/N7FK-XNEV]; James Vincent, *Google and Microsoft's Chatbots Are Already Citing One Another in a Misinformation Show*, VERGE (Mar. 22, 2023, 10:17 AM), https://www.theverge.com/2023/3/22/23651564/google-microsoft-bard-bing-chatbots-misinformation [https://perma.cc/7J5A-UU6H]; Maggie Harrison Dupré, *An AI Site Ripped Off Our Reporting About AI Ripoffs*, FUTURISM (Feb. 21, 2024, 12:33 PM), https://futurism.com/ai-ripped-off-reporting-ripoffs [https://perma.cc/V453-M4QF].

[47] 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 [https://perma.cc/7Q4L-5CQU].

[48] Donald Kimball, *Establishing an AI Task Force Is a Bad Idea*, WASH. POL'Y CTR. (Jan. 30, 2024),

purchasers and deployers of AI tools.[49] While their end goals differ from those of industry, their incentives to extract data and to shape people's behavior are broadly similar. And the line between governments and industry in AI is growing blurrier.[50]

In short, organizations deploying AI have overwhelming incentives to deploy sensors and screens into every aspect of our lives to collect and exploit everything they can for profit and power, starting with our data, labor, and attention. Right now, the law does little to stop them. One reason might be that people have become acclimated to it.

---

https://www.washingtonpolicy.org/publications/detail/establishing-an-ai-task-force-is-a-bad-idea [https://perma.cc/KF8P-U9N9] ("If, on the other hand, Washington's regulations are powerful enough to reach beyond state lines, we risk the national AI industry becoming secondary to other foreign powers."); Matt Berg & Rebecca Kern, *Ted Cruz: Congress 'Doesn't Know What the Hell It's Doing' with AI Regulation*, POLITICO (June 15, 2023), https://www.politico.com/news/2023/06/15/ai-ted-cruz-congress-00102116 [https://perma.cc/P5MS-7M9P] ("Washington can't allow itself to fall behind adversaries, particularly China, when it comes to implementing artificial intelligence in the military."). For critiques of this narrative, see, for example, Justin Sherman, *Reframing the U.S.-China AI "Arms Race"*, NEW AM. (Feb. 27, 2019), https://d1y8sb8igg2f8e.cloudfront.net/documents/Essay_Reframing_the_U.S.-China_AI_Arms_Race_2019-02-27_163939.pdf [https://perma.cc/LL2Y-2ZM8]; Meredith Whittaker et al., *China in Global Tech Discourse*, AI NOW INST. (May 27, 2021), https://ainowinstitute.org/publication/china-in-global-tech-discourse-2 [https://perma.cc/JK69-9EMK] ("The framing of the so-called US-China 'AI arms race' . . . is increasingly deployed to justify the expansion of large tech corporations' AI capabilities, while acting as a defense against critical work calling for restraint, reflection, and regulation of AI technologies and the firms behind them.").

[49] *See* Niklas Berglind et al., *The Potential Value of AI—and How Governments Could Look to Capture It*, MCKINSEY & CO. (July 25, 2022), https://www.mckinsey.com/industries/public-sector/our-insights/the-potential-value-of-ai-and-how-governments-could-look-to-capture-it [https://perma.cc/7R5D-DTCX].

[50] Michael German, *How Government Fusion Centers Violate Americans' Rights — and How to Stop It*, BRENNAN CTR. FOR JUSTICE (Dec. 15, 2022), https://www.brennancenter.org/our-work/analysis-opinion/how-government-fusion-centers-violate-americans-rights-and-how-stop-it [https://perma.cc/V6EU-WTFT].

II. We Will Get Used to It

By now you've likely noticed a predictable pattern in the deployment of AI tools. A company announces it's going to deploy a new AI tool, such as facial recognition in airports, emotion recognition in job interviews, or generative AI chatbots as therapists, that strikes many as "creepy."[51] Critics shout, companies assuage them, and upon encountering the tool for the first time, people wince a little. And then companies and governments just keep it up, slowly habituating everyone to their exposure and acclimating them to the idea that this is our new reality, so you might as well get used to it. Maybe lawmakers impose a few procedural hurdles like impact assessments, and a few people try to hold out. But like the smartphone, most of us are pushed to get on board sooner or later. Then, a company announces some new invasive tool, and the cycle repeats.

This is the technology normalization cycle, and unless lawmakers intervene, it is our fate.[52] We've long stopped

---

[51] Evan Selinger, *Why Do We Love to Call New Technologies "Creepy"?*, SLATE (Aug. 22, 2021, 3:30 AM), https://slate.com/technology/2012/08/facial-recognition-software-targeted-advertising-we-love-to-call-new-technologies-creepy.html [https://perma.cc/953R-MLL5]; Neil Richards, *"Creepiness" Is the Wrong Way to Think About Privacy*, SLATE (Dec. 2, 2021, 8:00 AM), https://slate.com/technology/2021/12/why-privacy-matters-excerpt-creepiness.html [https://perma.cc/TGM8-EP58]; Evan Selinger, *Health Care A.I. Needs to Get Real*, MEDIUM (Apr. 5, 2021), https://onezero.medium.com/health-care-a-i-needs-to-get-real-4aba0ae1241c [https://perma.cc/BHM9-GRQT]; Kif Leswing, *Microsoft's Bing A.I. is Producing Creepy Conversations with Users*, CNBC (Feb. 16, 2023), https://www.cnbc.com/2023/02/16/microsofts-bing-ai-is-leading-to-creepy-experiences-for-users.html; Chris Morris, *Snapchat's AI Could Be the Creepiest Chatbot Yet*, FAST CO. (Mar. 14, 2023), https://www.fastcompany.com/90865731/snapchat-ai-could-be-creepiest-chatbot-yet [https://perma.cc/A9E5-NNEP].

[52] *See also* Sarah Brayne, *The Banality of Surveillance*, 20 SURVEILLANCE & SOC'Y 372, 372 (2022); David Murakami Wood & Kirstie Ball, *Brandscapes of Control? Surveillance, Marketing and the Co-Construction of Subjectivity and Space in Neo-Liberal Capitalism*, 13 MKTG. THEORY 47 (2013); Gilles Deleuze, *Postscript on the Societies of Control*, 59 OCTOBER 3 (1992). *See*

noticing CCTV and many other surveillance tools as exceptional or out of place.[53] AI tools are next.[54] We're hastening our new normal of exposure with every new AI-powered device that we deploy in public, bring into our home, strap on our face, and put in our pocket.[55] Chris Gilliard calls

---

generally ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE (2013); JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE: SOCIAL CONTROL IN THE COMPUTER AGE (1974); SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA (2018); OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 31 (Oxford Univ. Press, 2d ed. 2021) (1993); DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW (2007); GARY T. MARX, WINDOWS INTO THE SOUL: SURVEILLANCE AND SOCIETY IN AN AGE OF HIGH TECHNOLOGY 114 (2016) (identifying four social processes in surveillance: "the *softening of surveillance*, meaning it becomes less visible and directly coercive, often being engineered into an activity; *patterns of expansion and contraction*, such as the tendency of a given means to quietly expand to new users and goals beyond those initially envisioned; *changes in surveillance* as social relationships change; and *stages of behavior* in the application of a tactic"); WILLIAM G. STAPLES, EVERYDAY SURVEILLANCE: VIGILANCE AND VISIBILITY IN POSTMODERN LIFE 5 (2d ed. 2013).

[53] Rebeca Santana & Rick Gentilo, *TSA Is Testing Facial Recognition at More Airports, Raising Privacy Concerns*, ASSOCIATED PRESS (May 15, 2023, 3:29 PM), https://apnews.com/article/facial-recognition-airport-screening-tsa-d8b6397c02afe16602c8d34409d1451f [https://perma.cc/W74Y-UF6K]; Benjamin Goold et al., *The Banality of Security: The Curious Case of Surveillance Cameras*, 53 BRIT. J. CRIMINOLOGY 977, 977 (2013).

[54] *See, e.g.*, Sofia Andrade, *Clear Wants to Scan Your Face at Airports. Privacy Experts Are Worried.*, WASH. POST (Dec. 20, 2023, 8:00 AM), https://www.washingtonpost.com/travel/2023/12/20/clear-facial-recognition-technology-airport-security [https://perma.cc/SJ8R-2AEX]; John Winner, *3 Tangible Ways that AI will Continue to Make Your Life Better*, FAST CO. (May 11, 2023), https://www.fastcompany.com/90892907/3-tangible-ways-that-ai-will-continue-to-make-your-life-better [https://perma.cc/F5SH-GBWV] ("In fact, AI already helps us in so many ways. . . . For instance, Face ID technology and the noise-cancellation feature on AirPods depend on AI to function. Plane and oil pipeline maintenance crews utilize AI to increase safety and uptime.").

[55] Chris Gilliard, *Amazon and the Rise of 'Luxury Surveillance'*, ATLANTIC (Oct. 18, 2022), https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772 [https://perma.cc/G8EN-SRKB]; Brayne,

this "luxury surveillance," and it will be our undoing.[56] In my work with Evan Selinger and Johanna Gunawan, we have argued that technology law too often "looks to people's expectations to set the limits of surveillance; yet over time, people become increasingly acclimated to being watched. People's desensitization to exposure affects how they view reasonable surveillance measures and fair tradeoffs."[57] By ignoring small, de minimis encroachments (what we call "privacy nicks" as compared to larger "privacy chops"), lawmakers encourage the normalization of harmful extractive and exploitative practices using AI tools.

Evan Selinger and Judy Rhee have highlighted two processes by which the initially "creepy" deployment of technology becomes normalized.[58] "*Unexceptional habituation* occurs when people in liberal Western democracies take ubiquitously encountered surveillance systems for granted—seeing them as so commonplace and mundane they are not worth thinking about critically."[59] The more a tool is deployed, the less remarkable it becomes as it fades into the background. When this happens, people often come to view a practice as acceptable, if not desirable, reflecting a psychological dynamic called "favorably disposed normalization."[60] The idea is that people often take moral cues from others' behavior, so observing routine behavior could signal that the technology is good.[61] There is also evidence that people come to rationalize their own use of a technology as desirable to avoid the difficult conclusion that they are acting wrongfully.[62]

---

supra note 52, at 372 (describing the progression of surveillance into society as "mundane . . . [q]uotidian . . . [b]anal . . . [and] more often than not, ordinary work done by ordinary people.").

[56] Gilliard, *supra* note 55.

[57] Hartzog et al., *supra* note 27, at 720.

[58] Evan Selinger & Judy Rhee, *Normalizing Surveillance*, 22 N. EUR. J. PHIL. 49, 49 (2021).

[59] Hartzog et al., *supra* note 27, at 762 (citing Selinger & Rhee, *supra* note 58).

[60] *Id.*

[61] Selinger & Rhee, *supra* note 58, at 59.

[62] *See generally, e.g.*, Justin P. Friesen et al., *System Justification: Experimental Evidence, Its Contextual Nature, and Implications for Social Change*, 58 BRIT. J. SOC. PSYCH. 315 (2018).

Perhaps you're thinking our eventual desensitization to AI is a good thing. That maybe our inevitable acclimation to being watched and exploited is proof that I'm overreacting. Proponents of AI (and "innovation" generally) often argue that critics have misjudged the risk of new digital tools.[63] They label concerns about technology as just the next "moral panic"—an unjustified fear of the new and unfamiliar.[64] The fact that people eventually stop objecting to these practices might be taken as evidence that they are harmless, if not desirable. This will probably be the case with certain technologies. People have now come to love many technology features which were once feared as "creepy," like Facebook's News Feed, caller ID, and turn-by-turn GPS directions.[65] If you

---

[63] Michael Schaus, *The Moral (and Political) Panic over Technology*, CREATIVE DISCOURSE (Aug. 29, 2023), https://creativediscourse.substack.com/p/the-moral-and-political-panic-over [https://perma.cc/Y3UD-PD6E]; John Herrman, *The Return of the Techno-Moral Panic*, N.Y. TIMES (Dec. 5, 2017), https://www.nytimes.com/2017/12/05/magazine/the-return-of-the-techno-moral-panic.html [https://perma.cc/JV32-BRHV]; Rich Haridy, *Concerns over Kids' Screen-Time a Modern-Day "Moral Panic", Says Study*, NEW ATLAS (Apr. 14, 2020), https://newatlas.com/science/screen-time-children-social-skills-moral-panic-kids-these-days [https://perma.cc/9VTV-3LLM]; Nicholas Bowman, *Banning Smartphones for Kids Is Just Another Technology-Fearing Moral Panic*, CONVERSATION (July 10, 2017, 9:05 PM), https://theconversation.com/banning-smartphones-for-kids-is-just-another-technology-fearing-moral-panic-74485 [https://perma.cc/RM8T-AF6Q]; Pamela Paul, *Do Not Panic. It's Just a Moral Panic*, N.Y. TIMES OPINION (June 29, 2023), https://www.nytimes.com/2023/06/29/opinion/columnists/moral-panic.html [https://perma.cc/7E4W-6JFY]; Marc Andreessen, *Why AI Will Save the World*, ANDREESSEN HOROWITZ (June 6, 2023), https://a16z.com/ai-will-save-the-world [https://perma.cc/8S6R-BCNT].

[64] Dan Milmo et al., *Nick Clegg Compares AI Clamour to 'Moral Panic' in the 80s over Video Games*, GUARDIAN (Oct. 31, 2020), https://www.theguardian.com/technology/2023/nov/01/nick-clegg-ai-clamour-similar-moral-panic-video-games [https://perma.cc/YB9U-E9NJ].

[65] John Leyden, *Users Protest over 'Creepy' Facebook Update*, REGISTER (Sept. 7, 2006), https://www.theregister.com/2006/09/07/facebook_update_controversy [https://perma.cc/DXB8-GB2D] ("'News Feed is just too creepy, too stalker-esque, and a feature that has to go'"); States News Service, '*Caller*

were to focus on your favorite examples, it might be easy to dismiss concerns of normalizing data collection and exploitation with AI as much ado about nothing.

But there's good reason to worry about the normalization of AI tools that extract our data and influence our lives. Just because people become desensitized to certain practices or even desire them does not mean they are harmless. As I wrote with Selinger and Gunawan, there are at least two reasons lawmakers should take a critical approach to society's acclimation to technology. First, by ignoring privacy nicks, lawmakers "create space for the constant infliction of autonomy harms that fail to meet the harm thresholds demanded by privacy rules."[66] Perhaps worse is the fact that the normalization cycle distorts and bypasses our collective ability to critically reflect on new AI deployments because our beliefs and dispositions about these tools are shaped by unconscious mental processes. This dynamic denies the public the ability to deliberate meaningfully on these tools before they become entrenched. And it leaves society particularly vulnerable when AI plays such a large role both in surveillance and in the misinformation and disinformation campaigns that undermine our basic social and political commitments.

The result is a version of the Collinridge Dilemma for AI policy, described by Ryan Calo:

> Try to intervene too soon, and policymakers risk misunderstanding the social impacts of emerging technology and hence doing more harm than good. Try to intervene too late, however, and technology will have already become intertwined in the fabric of everyday life. The policymaker then faces a public reliant upon the new

ID' Stirs Debate on Phone Privacy, N.Y. TIMES (Feb. 11, 1990), https://www.nytimes.com/1990/02/11/nyregion/caller-id-stirs-debate-on-phone-privacy.html [https://perma.cc/M7DJ-5T3N].

[66] Hartzog et al., *supra* note 27, at 724.

> affordances and a path dependent techno-social system that will be difficult to redirect.[67]

When it comes to AI and to surveillance in particular, Selinger, Gunawan, and I have argued that the law has been built to "allow society to constantly renegotiate its collective sense of reasonable expectations of privacy. The threshold for rejecting invasive new practices is perpetually being redrawn, excusing evermore invasive practices."[68] This will eventually lead to a disempowerment death spiral for democratic resistance because the law provides no backstop to normalization. Without better rules, the law will allow anything that people can be conditioned to tolerate. Because it happens incrementally, we are on track to tolerate everything. Democratic self-governance is simply not possible if people become so powerless and vulnerable that they can no longer conceive of rejecting a tool or practice.[69]

III. This Will Be Done "for Our Benefit"

It's easy to get excited about AI because companies and governments constantly hype it. With estimates suggesting that "artificial intelligence technologies could increase global GDP by $15.7 trillion, a full 14%, by 2030," it's hard to resist the urge to dive in headfirst.[70] The Biden administration has echoed the

---

[67] Ryan Calo, The Scale and the Reactor 22 (Apr. 9, 2022) (unpublished manuscript) (available at: https://ssrn.com/abstract=4079851 [https://perma.cc/C7GU-RKZP]). I've also heard scholars refer to this as "the Avocado ripeness problem": "Not yet . . . not yet . . . not yet . . . too late."

[68] Hartzog et al., *supra* note 27, at 724.

[69] *Id.* at 770.

[70] Darrell M. West & John R. Allen, *How Artificial Intelligence Is Transforming the World*, BROOKINGS INST. (Apr. 24, 2018), https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world [https://perma.cc/EG74-VVJ6]; *see also* Sundar Pichai & Demis Hassabis, *Introducing Gemini: Our Largest and Most Capable AI Model*, GOOGLE BLOG (Dec. 6, 2023), https://blog.google/technology/ai/google-gemini-ai/#sundar-note [https://perma.cc/8WGD-5E2T] ("Millions of people are now using generative AI across our products to do things they couldn't even a year

private sector's enthusiasm for AI, noting the technology's "potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure."[71] Compared to some of the more incremental, distributed, and delayed risks of AI, the large, individual, and immediate benefits are often staring us in the face.

This leads me to the third statement of this analytical exercise: the frequent lie that these AI tools are being developed and deployed "for us" and in our best interests. Of course, people will benefit from many of these new tools. But commercial development and deployments of AI are characterized by self-dealing—exploiting an advantage to benefit oneself rather than to benefit those exposing their data, labor, attention, and well-being.[72]

As a rule, self-dealing is expected and even desired as part of our economic system. For-profit companies owe no general obligation to act in the public good; their job is to maximize value for their owners and shareholders. But while self-dealing might be fine for standard, arms-length commercial exchanges, such as buying groceries or hiring a plumber, our relationship with companies deploying AI is uniquely imbalanced. We're on the bad end of an extreme power disparity and we've never been more vulnerable collectively or as individuals.[73] That

---

ago, from finding answers to more complex questions to using new tools to collaborate and create. At the same time, developers are using our models and infrastructure to build new generative AI applications, and startups and enterprises around the world are growing with our AI tools. This is incredible momentum, and yet, we're only beginning to scratch the surface of what's possible."); *BlenderBot 3: An AI Chatbot That Improves Through Conversation*, META (Aug. 5, 2022), https://about.fb.com/news/2022/08/blenderbot-ai-chatbot-improves-through-conversation [https://perma.cc/L556-LZY8] ("BlenderBot 3, a chatbot that can search the internet to talk about nearly any topic.").

[71] Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

[72] *Self-Dealing*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/self-dealing [https://perma.cc/4DGK-KDNM].

[73] *See, e.g.*, Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 996 (2022) ("The relationship between people and platforms has at least five traits that, when combined, make it highly imbalanced and worthy of intervention at the relational level: the

makes companies' overwhelming incentives for self-dealing in their relationships with us dangerous. When these companies use their power advantage to exploit the vulnerable, they act disloyally towards those that trusted them with their personal information, attention, labor, and well-being.[74] Three dynamics reveal how self-dealing makes a lie out of "AI for good": invitations of trust, incentives for exploitation, and the adverse consequences of self-dealing.

First, to profit, industry needs you to trust their claims that AI will benefit you. Part of this is easy, because AI has a hold on our collective imagination, priming us to believe it's capable of anything from companionship to human extinction.[75] It feels like the stuff of science fiction and draws upon the idea that in the public consciousness, "[a]ny sufficiently advanced technology is indistinguishable from magic."[76] Companies can seize upon this to market the benefits of AI systems.

---

relationship (1) is ongoing, (2) is high frequency, (3) occurs within an interactive environment, (4) operates within an environment completely constructed for the individual, and (5) operates within an environment that is responsive to the individual by the dominant party.").

[74] *See, e.g.*, Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021) [hereinafter Richards & Hartzog, *Duty of Loyalty*]; Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180 (2017) [hereinafter Richards & Hartzog, *Trust Gap*]; Woodrow Hartzog & Neil Richards, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579 (2017); Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 6 EUR. DATA PROT. L. REV. 492 (2020); Hartzog & Richards, *supra* note 73; Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022) [hereinafter Hartzog & Richards, *Data Loyalty*].

[75] *See* Ryan Calo, *Artificial Intelligence and the Carousel of Soft Law*, 2 IEEE TRANSACTIONS ON TECH. & SOC'Y 171, 172 (2021) [hereinafter Calo, *Carousel*]; Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 402 (2017); Michael Atleson, *Keep Your AI Claims in Check*, FED. TRADE COMM'N: BUS. BLOG (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check [https://perma.cc/N2KW-YXPY].

[76] Efraín Foglia et al., *"Any Sufficiently Advanced Technology Is Indistinguishable from Magic."*, CENTRE DE CULTURA CONTEMPORÀNIA DE BARCELONA (Nov. 8, 2018), https://lab.cccb.org/en/arthur-c-clarke-any-sufficiently-advanced-technology-is-indistinguishable-from-magic [https://perma.cc/3VHM-RRQ7].

Companies deploying AI say they are acting in the public good.[77] But there's good reason to be skeptical of these platitudes and of their general commitment to "ethical AI principles." Ethical principles are poor substitutes for laws and can even delay eventual rules because espousing principles and pointing to ethics committees can give the illusion of progress. It's easy to say you're acting for the public good without losing any money.[78] Google has long since excised "don't be evil" from its code of conduct, and OpenAI only lasted four years in "service of humanity" before needing to turn a profit.[79] Even when companies purport to serve us, they use the need to train AI to justify taking an excessive amount of data.

---

[77] *OpenAI Charter*, OPENAI (Apr. 9, 2018), https://openai.com/charter; *AI For Good Lab*, MICROSOFT, https://www.microsoft.com/en-us/research/group/ai-for-good-research-lab; *Applying AI to Make a Difference in the Lives of Those Who Need It Most*, GOOGLE AI https://ai.google/responsibility/social-good [https://perma.cc/RW8G-VHBE].

[78] Calo, *Carousel*, *supra* note 75, at 173 ("The impulse of so many organizations across nearly every sector of society to promulgate principles in response to the ascendance of AI is understandable. Unlike law, which requires consensus and rigid process, an organization can develop and publish principles unilaterally . . . and while common principles can lay a foundation for societal change, they are no substitute for law and official policy. . . . No invisible hand guides market participants to charity. The Internet is not Eden. Uber and Airbnb are not sharing with anyone. And AI is not a magical genie-in-training. . . . The role of the law is to understand, channel, and address that change—with rules, not aspirations.").

[79] Kate Conger, *Google Removes 'Don't Be Evil' Clause from Its Code of Conduct*, GIZMODO (May 18, 2018), https://gizmodo.com/google-removes-nearly-all-mentions-of-dont-be-evil-from-1826153393 [https://perma.cc/YL9A-AUGC] ("The updated version of Google's code of conduct still retains one reference to the company's unofficial motto—the final line of the document is still: 'And remember . . . don't be evil, and if you see something that you think isn't right – speak up!'"); *OpenAI Charter*, *supra* note 77; Chinecherem Nduka, *The Transformation of OpenAI from Nonprofit to $29B For-Profit*, SOCIABLE (Apr. 5, 2023), https://www.sociable.co/business/the-transformation-of-openai-from-nonprofit-to-29b-for-profit [https://perma.cc/W4WF-NM49]; Kelsey Piper, *Why the World's Leading AI Charity Decided to Take Billions from Investors*, VOX (Apr. 17, 2019), https://www.vox.com/future-perfect/2019/4/17/18301070/openai-greg-brockman-ilya-sutskever [https://perma.cc/7AHN-TSLG].

The second feature that encourages companies to use AI systems for self-dealing is the tools' affordances for exploitation. Because AI systems are often "plug and play" into other services and devices, it is easy for companies to market the benefit of a new AI affordance as a pretext for capturing our data, attention, and labor. With a vendor contract or just a few flipped switches, facial recognition can be deployed in IoT devices; generative AI can be deployed in social media and in text and image creation tools to create deepfakes, and voice recognition can be easily deployed in Wendy's drive-thrus.[80]

Exploitation is most likely when AI is combined with platforms that have remarkable affordances for extraction and just enough of a value proposition to drive adoption. Companies offer up chatbots as educators and delivery robots on college campuses with little care or concern about whether these services will be, on balance, beneficial or even needed.[81] Self-dealing is not limited to AI, of course. Other companies that depend on our data, like those dealing with our genetic data, also look to exploit our information for profit.[82] AI also "democratizes" exploitation by reducing the cost and expertise necessary to fleece millions.[83] Actors can easily use AI to

---

[80] *AI and Beyond: Wendy's New Innovative Restaurant Tech,* WENDY'S BLOG (June 2, 2023), https://www.wendys.com/blog/how-wendys-using-ai-restaurant-innovation [https://perma.cc/G82G-XTGR].

[81] Natasha Singer, *Will Chatbots Teach Your Children?*, N.Y. TIMES (Jan. 11, 2024), https://www.nytimes.com/2024/01/11/technology/ai-chatbots-khan-education-tutoring.html [https://perma.cc/F8RJ-35GS]; Koebler, *supra* note 44.

[82] Thomas Germain, *23andMe Admits 'Mining' Your DNA Data Is Its Last Hope"*, GIZMODO (Feb. 13, 2024, 2:30 PM), https://gizmodo.com/23andme-admits-mining-your-dna-data-is-its-last-hope-1851252582 [https://perma.cc/4M82-R29Y].

[83] *See* Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81, 82 (2013); Press Release, Federal Trade Commission, FTC Proposes New Protections to Combat AI Impersonation of Individuals (Feb. 15, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals [https://perma.cc/472N-XH6B].

deceive people, and fraud is just the beginning of the kind of turnkey exploitation afforded by AI tools.[84]

Third, companies make a lie out of "AI for good" because they so commonly will use these tools to harm us. Companies use AI to save time and money while polluting the Internet with fake imagery and false information.[85] Companies also consume massive amounts of resources with huge environmental effects, often for dubious, speculative, or modest gains.[86] Some of the AI doomers speculate about a kind of sentient superintelligence that spells the end of humanity, but the more likely scenario is that devastating climate change will decimate and disrupt human civilization long before we

---

[84] Michael Atleson, *The Luring Test: AI and the Engineering of Consumer Trust*, FED. TRADE COMM'N: BUS. BLOG (May 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust [https://perma.cc/F4LJ-4D5P].

[85] Emanuel Maiberg, *Instacart's AI Recipes Look Literally Impossible*, 404 MEDIA (Feb. 21, 2024, 8:50 AM), https://www.404media.co/instacarts-ai-recipes-look-literally-impossible [https://perma.cc/9ZHL-9E9R]; Pranshu Verma, *The Rise of AI Fake News Is Creating a 'Misinformation Superspreader'*, WASH. POST (Dec. 17, 2023, 6:00 AM), https://www.washingtonpost.com/technology/2023/12/17/ai-fake-news-misinformation [https://perma.cc/9RWD-7CYC]; Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1763 (2019); Caroline Mimbs Nyce, *AI Search Is Turning into the Problem Everyone Worried About*, ATLANTIC (Nov. 6, 2023), https://www.theatlantic.com/technology/archive/2023/11/google-generative-ai-search-featured-results/675899 [https://perma.cc/58TG-4KDJ].

[86] *The Climate Costs of Big Tech*, AI NOW INST. (Apr. 11, 2023), https://ainowinstitute.org/spotlight/climate [https://perma.cc/K84A-U6W4]; CRAWFORD, *supra* note 4, at 15; Mary K. Pratt, *Generative AI's Sustainability Problems Explained*, TECHTARGET (Oct. 20, 2023), https://www.techtarget.com/sustainability/feature/Generative-AIs-sustainability-problems-explained [https://perma.cc/QPP3-Z59C]; Kate Crawford & Vladen Joler, *Anatomy of an AI System*, ANATOMY AI SYS. (2018), https://anatomyof.ai [https://perma.cc/2UX6-UBHT]; Payal Dhar, *The Carbon Impact of Artificial Intelligence*, 2 NATURE MACH. INTEL. 423 (2020); Steven Gonzalez Monserrate, *The Staggering Ecological Impacts of Computation and the Cloud*, MIT PRESS READER (Feb. 14, 2022), https://thereader.mitpress.mit.edu/the-staggering-ecological-impacts-of-computation-and-the-cloud [https://perma.cc/2FXR-X3JA].

need to worry about robots becoming "self-aware."[87] If AI systems are used for existential harm, industry—not some runaway automation—will be the engine, and governments will be contributing or asleep at the wheel.[88]

In the meantime, companies push ineffective technological solutions to such complex social problems as inequality and loneliness, which need labor and love, not artifacts and artifice.[89] Of course, all this assumes that the AI tools being sold actually can do what they are marketed to do. Companies too often sell AI models that they know don't work, compounding the harm to people and recklessly and callously turning society into their testing ground.[90]

---

[87] *See* Roel Dobbe & Meredith Whittaker, *AI and Climate Change: How They're Connected, and What We Can Do About It*, AI NOW INST. (Oct. 17, 2019), https://ainowinstitute.org/publication/ai-and-climate-change-how-theyre-connected-and-what-we-can-do-about-it [https://perma.cc/CKE5-DTWU]; Jude Coleman, *AI's Climate Impact Goes Beyond Its Emissions*, SCI AM (Dec. 7, 2023), https://www.scientificamerican.com/article/ais-climate-impact-goes-beyond-its-emissions [https://perma.cc/6W4W-SPSE]; Tamara Kneese, *Climate Justice and Labor Rights | Part I: AI Supply Chains and Workflows*, AI NOW INST. (Aug. 2, 2023), https://ainowinstitute.org/general/climate-justice-and-labor-rights-part-i-ai-supply-chains-and-workflows [https://perma.cc/57SU-WZH7]; *see also* Toby Walsh, *Elon Musk Is Wrong. The AI Singularity Won't Kill Us All*, WIRED (Sept. 20, 2017, 3:00 AM), https://www.wired.com/story/elon-musk-artificial-intelligence-scaremongering [https://perma.cc/F8K8-HRCN].

[88] Dan Milmo, *AI Risk Must Be Treated as Seriously as Climate Crisis, Says Google DeepMind Chief*, GUARDIAN (Oct. 24, 2023, 8:00 EDT), https://www.theguardian.com/technology/2023/oct/24/ai-risk-climate-crisis-google-deepmind-chief-demis-hassabis-regulation [https://perma.cc/5VG5-UP2H]; Will Daniel, *The 'Godfather of A.I.' Says His Technology Is a Bigger Threat Than Climate Change: 'It's Not at all Clear What You Should Do'*, FORTUNE (May 8, 2023, 2:13 PM EDT), https://fortune.com/2023/05/08/godfather-artificial-intelligence-geoffrey-hinton-climate-change [https://perma.cc/Q6P5-ELN5].

[89] Thomas Germain, *Your AI Girlfriend Is a Data-Harvesting Horror Show*, GIZMODO (Feb. 14, 2024), https://gizmodo.com/your-ai-girlfriend-is-a-data-harvesting-horror-show-1851253284 [https://perma.cc/7QZU-2WX7].

[90] Belle Lin, *Google and Anthropic Are Selling Generative AI to Businesses, Even as They Address Its Shortcomings*, WALL ST. J. (Feb. 13, 2024, 7:00 AM EST), https://www.wsj.com/articles/google-and-anthropic-are-selling-generative-ai-to-businesses-even-as-they-address-its-shortcomings-ff90d83d [https://perma.cc/P5SB-3LT5]; Hasan Chowdhury, *ChatGPT Has*

Industry's promise that AI will benefit us also too often ignores the fact that not all groups benefit from these tools equally. Traditionally marginalized groups are particularly vulnerable, exploited, and excluded. AI systems are notoriously, and perhaps inevitably, biased. Many scholars have spent decades identifying the ways in which AI systems are biased against marginalized and underrepresented communities, most notably along the familiar lines of race, class, gender, and ability.[91] Of course, bias in AI is just a symptom of a larger problem about how power is amassed and wielded against marginalized communities.[92] But that's the rub: even if industry ensures that AI systems work equally well for all communities, they will have still created systems that will likely be used to dominate, damage, misinform, manipulate,

---

Been Losing Its Mind and No One Seems to Know Why, BUS. INSIDER (Feb. 21, 2024, 10:12 AM EST), https://www.businessinsider.com/chatgpt-giving-users-unhinged-answers-no-one-knows-why-openai-2024-2 [https://perma.cc/7ST8-GGB4].

[91] *See generally, e.g.*, AJUNWA, *supra* note 19; BROUSSARD, MORE THAN A GLITCH, *supra* note 4; SAFIA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018); RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE (2019); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018); CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016); SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS (2015); CRAWFORD, *supra* note 4; Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*, 14 ACM TRANSACTIONS ON INFO. SYS. 330 (1996); Aylin Caliskan, Joanna J. Bryson & Arvind Narayanan, *Semantics Derived Automatically from Language Corpora Contain Human-Like Biases*, 356 SCIENCE 183 (2017); Muhammad Ali et al., *Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes*, 3 PROC. ACM ON HUM.-COMPUT. INTERACTION, Nov. 7, 2019, at 1; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* 1 (2018); Ngozi Okidegbe, *Discredited Data*, 107 CORNELL L. REV. 2007 (2022).

[92] *See* Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 132 YALE L.J. F. 907, 910 (2022) (noting that the experiences of African Americans online are compounded by existing vulnerabilities such as "excessive and discriminatory surveillance," "targeted exclusion through differential access to online opportunities," and "exploitative online financial fraud and deception").

and discriminate. Even AI tools designed to *mitigate* bias and wrongful discrimination will be ineffective or harmful in the hands of companies and governments with contrary incentives.

Companies offering AI tools ostensibly designed to make labor more efficient conveniently ignore the likelihood that these tools will make employees' lives worse. Companies are more likely to use them simply to raise the bar for how hard people must work, further exacerbating inequalities and only benefiting those who already have all the power.[93] Companies leverage vague and selective notions of AI "innovation" to tempt politicians and the populace, but that rhetoric has become so overhyped and talismanic that it now feels like shorthand for "let me do what I want or else."[94] Neil Richards has criticized the rhetoric around innovation as selectively vague, meaning it can be whatever a technology company wants it to be, and to hear them tell it, innovation is always good and never bad.[95] This slippery notion of innovation also has the strength of convenience—when advertising the latest product launch, innovation seems like a supernatural force.

---

[93] *See, e.g.*, AJUNWA, *supra* note 19, at 4 (describing AI in the workplace as the latest high-tech iteration of a robust history of "worker subjugation through quantification"); Viktoria Tomova, *AI Solutions for Domestic Labor May Exacerbate Inequities*, TECH POLICY PRESS (Feb. 21, 2024), https://www.techpolicy.press/ai-solutions-for-domestic-labor-may-exacerbate-inequities [https://perma.cc/L9L5-LQJD]; Rashi Shrivastava, *Dozens of KFC, Taco Bell and Dairy Queen Franchises Are Using AI to Track Workers*, FORBES (Feb. 23, 2024, 6:30 AM EST), https://www.forbes.com/sites/rashishrivastava/2024/02/23/dozens-of-kfc-taco-bell-and-dairy-queen-franchises-are-using-ai-to-track-workers [https://perma.cc/D5PN-SN6P].

[94] *See* NEIL RICHARDS, WHY PRIVACY MATTERS 177 (2021) ("[H]ere's an experiment: take any sentence from a technology company about 'innovation,' and replace the word 'innovation' with 'magic' to see if the meaning of the sentence changes at all. In my own experience playing this game many times over the past decade, it almost never changes the meaning."); *see also* JESSICA SILBEY, AGAINST PROGRESS: INTELLECTUAL PROPERTY AND FUNDAMENTAL VALUES IN THE INTERNET AGE 5 (2022) (arguing that in the Twentieth Century, industry largely equated "progress" in the innovation sense with simply "more").

[95] RICHARDS, *supra* note 94, at 179 ("The rhetorical construction of 'innovation' by the tech sector slices off everything bad and leaves only the gleaming stainless steel of a technological utopia, one that is all Thomas More and no George Orwell.").

But the moment regulation is proposed, innovation becomes easily "stifled," as fragile as a house of cards, toppled by the slightest legal obligation.[96] It's the ideal tool for convincing people to get excited about extractive business models.

In short, our relationship with technology companies is so uniquely exposed and imbalanced that it is a betrayal when companies exploit our vulnerabilities for profit. These betrayals undermine the interpersonal trust, institutional trust, and social trust necessary for a thriving society.[97] There are many reasons why public trust in professions and institutions is already near an all-time low, but it's clear that technology platforms and companies building and deploying AI-driven systems are part of the problem.[98] And efforts to remedy this

---

[96] *Id.* at 179-80.

[97] *See generally, e.g.*, ROBERT D. PUTNAM, BOWLING ALONE: THE COLLAPSE AND REVIVAL OF AMERICAN COMMUNITY (2001); BRUCE SCHNEIER, LIARS AND OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE (2012); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016).

[98] *See Public Trust in Government: 1958-2023*, PEW RSCH. CTR. (Sept. 19, 2023), https://www.pewresearch.org/politics/2023/09/19/public-trust-in-government-1958-2023 [https://perma.cc/S4VL-8GSK]; Sara Lebow, *Social Users Don't Trust Facebook*, EMARKETER (Oct. 13, 2022), https://www.emarketer.com/content/social-users-trust-facebook [https://perma.cc/F76B-PR2B]; Chloe Berger, *Disillusioned Americans are Losing Faith in Almost Every Profession*, FORTUNE (Feb. 5, 2024, 4:43 PM EST), https://fortune.com/2024/02/05/disillusioned-americans-losing-faith-ethics-professions-jobs-trust [https://perma.cc/QX6V-ZPRL]; Ina Fried, *Americans' Trust in Tech Companies Hits New Low*, AXIOS (Apr. 7, 2022), https://www.axios.com/2022/04/07/trust-tech-companies-new-low-americans [https://perma.cc/9MAU-GRKT]; Paul Barrett et al., *How Tech Platforms Fuel U.S. Political Polarization and What Government Can Do About It*, BROOKINGS INST. (Sept. 27, 2021), https://www.brookings.edu/articles/how-tech-platforms-fuel-u-s-political-polarization-and-what-government-can-do-about-it [https://perma.cc/K4Z7-XQUP]; *see generally* FRANCESCA BOLLA TRIPODI, THE PROPAGANDISTS' PLAYBOOK: HOW CONSERVATIVE ELITES MANIPULATE SEARCH AND THREATEN DEMOCRACY (2022) (exploring how conservative elites, politicians, and media pundits wield the power created and distributed by search engines to promote their agenda and divert public attention away from news unflattering to conservative campaigns).

problem aren't working.[99] Meanwhile, people can't stop proclaiming the death of privacy as a deep fatalism and resignation settles in right as the AI boom begins.[100]

The pursuit of profit over people is why many new AI tools feel like a solution in search of a problem.[101] Mix in techno-solutionism, which offers up technological solutions for complex social and political problems, and you're on the path to misery.[102] If you think self-checkout machines are annoying and counterproductive, just wait until you are denied a human therapist, tutor, or tax professional in favor of a chatbot.[103]

---

[99] *See* Will Oremus, *The Biggest Online Threat to 2024 Elections Isn't AI*, WASH. POST (Feb. 14, 2024, 9:26 AM EST), https://www.washingtonpost.com/politics/2024/02/14/biggest-online-threat-2024-elections-isnt-ai [https://perma.cc/83VN-V5M9].

[100] Selinger & Hartzog, *supra* note 7.

[101] Panu Korhonen, *AI Is a Solution in Search of a Problem*, MEDIUM (Feb. 2, 2023), https://uxdesign.cc/ai-is-a-solution-in-search-of-a-problem-ab4c6e818206 [https://perma.cc/4ZD7-YYNK]; Wojciech Wiewiórowski, *Facial Recognition: A Solution in Search of a Problem?*, EUROPEAN DATA PROT. SUPERVISOR: BLOG (Oct. 28, 2019), https://www.edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en [https://perma.cc/87U9-BMV8]; Joshua A. Kroll, *Why AI Is Just Automation*, BROOKINGS INST. (July 14, 2021), https://www.brookings.edu/articles/why-ai-is-just-automation [https://perma.cc/LEP9-69HT] ("Too often, the promise of new and automated versions of manual processes leads to a rush to deploy solutions without regard to how the new order of operations will affect the full range of stakeholders or how a new tool will integrate into systems and organizations. The mere existence of technology becomes a solution in search of a problem, with management setting implementation goals like 'use AI' or 'make decisions in a data-driven way' without first establishing a problem to which these tools may productively be applied.").

[102] *See, e.g.*, Greta Byrum & Ruha Benjamin, *Disrupting the Gospel*, STAN. SOC. INNOVATION REV. (June 16, 2022), https://ssir.org/articles/entry/disrupting_the_gospel_of_tech_solutionism_to_build_tech_justice [https://perma.cc/67ZG-UUXE]. This is not a new problem or observation. But it is a persistent one. *See also* Ian Tucker, *Evgeny Morozov: 'We Are Abandoning All the Checks and Balances'*, GUARDIAN (Mar. 9, 2013, 2:20 PM EST), https://www.theguardian.com/technology/2013/mar/09/evgeny-morozov-technology-solutionism-interview [https://perma.cc/UHG2-TCEA].

[103] Amanda Mull, *Self-Checkout Is a Failed Experiment*, ATLANTIC (Oct. 18, 2023), https://www.theatlantic.com/technology/archive/2023/10/self-

So far, AI tools are primarily driving data markets and data refineries that, in the words of Julie Cohen, aren't being deployed to reveal a deeper understanding of ourselves "but rather predictability in pursuit of profit."[104] Industry will take advantage of every opportunity so that our future behavior can be more reliably predicted and influenced for ongoing extraction and exploitation.[105] Companies are already deploying AI surveillance for cheaper and more effective micromanagement of tasks to make life miserable for low-wage employees.[106] The driving force of industry's implementation of new technology has always been to sell things and cut costs—and AI is no exception.[107]

---

checkout-kiosks-grocery-retail-stores/675676 [https://perma.cc/SLW6-PGFD]; Evan Selinger, *We Don't Want Chatbots to Come Off as People*, BOS. GLOBE (May 8, 2023, 3:00 AM), https://www.bostonglobe.com/2023/05/08/opinion/google-bard-chatgpt-dishonest-anthropomorphism-evan-selinger [https://perma.cc/6N6U-GD99]; Lauren Aratani, *US Eating Disorder Helpline Takes Down AI Chatbot Over Harmful Advice*, GUARDIAN (May 31, 2023, 2:55 PM EST), https://www.theguardian.com/technology/2023/may/31/eating-disorder-hotline-union-ai-chatbot-harm [https://perma.cc/CWS8-2ZK3]; Geoffrey A. Fowler, *TurboTax and H&R Block Now Use AI for Tax Advice. It's Awful.*, WASH. POST (March 4, 2024, 8:00 AM EST), https://www.washingtonpost.com/technology/2024/03/04/ai-taxes-turbotax-hrblock-chatbot [https://perma.cc/JQ4C-TCGW]; Beatrice Nolan, *Klarna Says Its AI Assistant Is Doing the Work of 700 People After Putting the Brakes on Hiring*, BUS. INSIDER (Feb. 28, 2024, 9:47 AM EST), https://www.businessinsider.com/klarna-ai-chatbot-work-700-people-2024-2 [https://perma.cc/Z9ZG-BZFQ].

[104] COHEN, *supra* note 6, at 71; *see also id.* ("Data refineries are designed to offer powerful, high-speed techniques for matching populations with particular strategies calibrated for surplus extraction. The techniques operate on 'raw' personal data to produce 'refined' data doubles and use the data doubles to generate preemptive nudges that, when well executed, operate as self-fulfilling prophecies, eliciting the patterns of behavior, content consumption, and content sharing already judged most likely to occur.").

[105] *Id.* ("Such operations have a very particular economic purpose: They work to maintain and stabilize the available pool of consumer surplus so that it may be more reliably identified and easily extracted.").

[106] *See, e.g.*, Shrivastava, *supra* note 93.

[107] *See* Ashley Belanger, *Air Canada Must Honor Refund Policy Invented by Airline's Chatbot*, ARS TECHNICA (Feb. 16, 2024, 12:12 PM),

AI tools might benefit us, but they will not be created for our collective benefit. This distinction matters because the affordances of AI that can benefit people so often come bundled with a host of hidden evils. People might easily understand the purported benefits of these tools but miss the harms to themselves and others. Often, AI tools that collect large amounts of personal information will be little more than a hidden data grab dressed up as a modest distraction or a solution to an inconvenience.[108] While such tools might be desirable, the rampant self-dealing inherent in the development and deployment of these systems threatens to turn any application of an AI system into a mousetrap filled with cheese.

Industry does not have the incentive to consider whether a deployment of AI will isolate us, atrophy our skills, wrongfully discriminate against us, displace our time and labor, cause us to be exposed, or poison our public discourse and weaken democracy. If they can legally sell it to us for a profit, that's enough justification for funders and the C-suite. As individual consumers, we probably don't fully consider all these dangers either.[109] We're just not built for complex threat modeling when standing at the cash register. That means it is up to us collectively, as citizens and members of society, to ensure the juice is worth the squeeze.

---

https://arstechnica.com/tech-policy/2024/02/air-canada-must-honor-refund-policy-invented-by-airlines-chatbot [https://perma.cc/3UXT-M8DN].

[108] *See* Office of Technology & Division of Privacy and Identity Protection, *AI (and Other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive*, FED. TRADE COMM'N: TECH. BLOG (Feb. 13, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive [https://perma.cc/4RSZ-3ARZ].

[109] *See generally* NANCY S. KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019); Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33 (2020); Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573 (2021); Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385 (2015).

IV. The Way Forward: The Four "D's" of AI Regulation

For starters, successfully regulating AI requires a robust and effective administrative state, the ability for individuals to bring causes of action against culpable companies, an approach to free expression focused on people and not on profit, and the political will and ability to enforce the rules we've already got.[110] But that's true far beyond AI. If government and the people lose the ability to hold organizations accountable, we're toast anyway.

The two AI truths and a lie are also part of a bigger story about technology and corporate greed. There are several different accounts of this story. Kate Crawford explains AI's extractive nature by reference to the capitalist-colonial logics of classification that underpin it.[111] Shoshana Zuboff sees digital extraction as the inevitable endgame of late capitalism.[112] Julie Cohen sees digital platform extraction and manipulation as a way to remake social and political institutions to legitimize their financial gain.[113] AI is just the latest tool to succumb to what Cory Doctorow has called the "enshittification" of digital platforms.[114] Doctorow describes the inevitable degradation cycle of platforms as "first, they are good to their users; then they abuse their users to make things better for their business customers; finally, they abuse those business customers to claw back all the value for themselves. Then, they die."[115] Under this theory, companies deploying AI will try to avoid the four forces that discipline companies:

---

[110] *See* Calo, *Carousel*, *supra* note 75, at 171 ("[U]ltimately what is missing is not knowledge about the content of ethics as much as political will. If, as both detractors and proponents claim, AI constitutes the transformative technology of our time, then one of the aspects of society that must transform is the law and legal institutions.").

[111] CRAWFORD, *supra* note 4, at 62.

[112] ZUBOFF, *supra* note 20, at 518-19.

[113] COHEN, *supra* note 6, at 6-7.

[114] Cory Doctorow, *The 'Enshittification' of TikTok*, WIRED (Jan. 23, 2023, 12:44 PM), https://www.wired.com/story/tiktok-platforms-cory-doctorow [https://perma.cc/GT3B-GFG6].

[115] Cory Doctorow, *TikTok's Enshittification*, CRAPHOUND.COM (Feb. 20, 2023), https://craphound.com/news/2023/02/20/tiktoks-enshittification [https://perma.cc/CFQ7-85ZW].

competition, regulation, self-help, and workers. Any holistic regulatory response to AI and the broader story of technology and corporate greed must embolden these forces, or else the cycle will continue.

Because AI is not a monolith and affects so many different aspects of society, a comprehensive approach to AI should include a robust antitrust and competition-law response, a reckoning with AI's enormous environmental impact, and a coherent and integrated response from any legal framework that is already grappling with the affordances of digital technologies, such as health law, labor and employment law, intellectual property, torts, contracts, and more.

But in this Part, I'll focus on the area of law most directly affected by the AI pathologies of extraction, normalization, and self-dealing: information rules. If it is true that the AI industry will take and use all the data it can for its own benefit and that we will eventually get used to it, then lawmakers will need to change their usual approach to regulating information and technology. Procedural approaches requiring transparency and consent will not be enough. People can be conditioned and manipulated into agreeing to harmful practices. Transparency that doesn't spur action from a desensitized population only further justifies wrongful conduct. Co-regulatory approaches and rules that provide too much wiggle room for industry should also be suspect because companies have an overwhelming incentive to ensure that all rules and enforcement leave their business models intact, even if those models are harmful and exploitative.[116] Finally, lawmakers should get serious about outright prohibitions on collecting data. Merely regulating use of data ignores how information collection and the affordances of tools bestow, distribute, and exercise power.

Instead of transparency, consent, self-regulation, and limiting uses of AI, lawmakers should embrace a strategy of duties, design rules, defaults, and data-collection dead ends for

---

[116] *See* WALDMAN, *supra* note 6, at 233 (advocating for stricter and more effective legal constraints, including rules that directly regulate substance); COHEN, *supra* note 6, at 269, 270 (noting that "countermovements are inevitably temporary" but have "invited new strategies for evasion, capture, co-optation, and arbitrage").

data processing and deployments of AI. This layered approach will more squarely address data extraction, normalization, and self-dealing and better ensure that research and development into AI advances the public good. Duties will limit self-dealing by prioritizing people over profit and will help ensure that humans are protected no matter what they choose. Design rules will help ensure that companies don't launder moral responsibility for their creations under some false notion of tech neutrality. Defaults will better limit data collection to what is necessary and desired, creating a presumption against treating people as a freely exploitable resource. Finally, data dead ends will provide a clear and substantive backstop to resist normalizing exploitation and the false narrative that all technologies and data practices are inevitable.

1. Duties

Consent is one of the first things lawmakers reach for when creating information rules. But not only is valid consent impossible in mediated environments, consent also normalizes extractive practices and self-dealing by providing legal and moral justification.[117] Consent is a broken regulatory approach to technology at scale. It is illusory, overwhelming, and myopic.[118] What are needed are non-negotiable duties that bind actors to responsible and loyal behavior so that people are protected no matter what they choose. Neil Richards and I have argued that lawmakers should create duties of loyalty for companies entrusted with people's information and technologically mediated experiences.[119]

Data loyalty is the simple idea that the organizations we trust should not process our data or design their tools in ways that conflict with our best interests. It borrows from notions of

---

[117] *See, e.g.*, Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1486-90 (2019).

[118] Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 426-30 (2018); HARTZOG, *supra* note 5, at 63-64.

[119] *See, e.g.*, Richards & Hartzog, *Duty of Loyalty*, *supra* note 74; Hartzog & Richards, *supra* note 73; Hartzog & Richards, *Data Loyalty*, *supra* note 74; Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020); Richards & Hartzog, *supra* note 97; Richards & Hartzog, *supra* note 117; Richards & Hartzog, *Trust Gap*, *supra* note 74.

loyalty in fiduciary law, but it is distinct from them. The model we propose would be crafted by legislators to the specific vulnerabilities and incentives in the relationship between consumers and the data-extractive companies they deal with every day.

Scholars have proposed duties of loyalty in a variety of forms—including loyalty duties for data collectors, "information fiduciaries," or fiduciary boilerplate—in part because loyalty represents a substantive check on the ability of companies to use human data to nudge, influence, coerce, and amass vast profits from the exploitation of human information.[120] Richards and I have argued that data loyalty "cannot be avoided by trickery, hidden fine print, or manipulative interfaces known as 'dark patterns.' At its core, it

---

[120] *See, e.g.*, Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Anthony Aguirre et al., *AI Loyalty by Design: A Framework for Governance of AI*, *in* THE OXFORD HANDBOOK OF AI GOVERNANCE 320 (Justin B. Bullock et al. eds. 2022); Lauren Henry Scholz, *Fiduciary Boilerplate, Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143 (2020). *See generally* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34 (2020); Lilian Edwards, *Reconstructing Consumer Privacy Protection On-Line: A Modest Proposal*, 18 INT'L REV. L. COMPUTS. & TECH. 313 (2004); Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95 (2019); Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 340 (2014); Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057 (2019); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1 (2018); Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game [https://perma.cc/5LFT-CV9L]; Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419 (2001); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004); Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 SANTA CLARA HIGH TECH. L.J. 75 (2019); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015).

protects the expectations consumers bring to relationships with companies, and it builds trust in those relationships that allows them to flourish to the benefit of both parties."[121] We wrote:

> A duty of loyalty for privacy law is neither perfect nor a tool for all tasks. But loyalty has one great virtue: it places the focus for information age problems on the relationships that define our social lives rather than on the data which is the byproduct of those relationships. Loyalty shifts the law's attention from the procedural rules of privacy law that are too easy to manipulate . . . to the substantive question of what practices go too far. It is flexible and adaptable across contexts, cultures, and times.[122]

We proposed that lawmakers use a two-step process to (1) articulate a primary, general duty of loyalty for those deploying AI, then to (2) articulate "subsidiary" duties that are more specific and sensitive to context.[123] Subsidiary duties regarding collection, personalization, gatekeeping, persuasion, and mediation would target the most opportunistic contexts for self-dealing and result in flexible open-ended duties combined with highly specific rules. In the AI context, some important specific rules include a robust data minimization obligation, anti-subordination provisions, and prohibitions on secondary uses and third-party disclosure of personal data, including biometric data and cross-context behavioral advertising.

In addition to a duty of loyalty, lawmakers should codify and embolden a duty of care on all companies developing and deploying AI systems. Such a duty would protect against companies creating an unreasonable risk of harm to others. In theory, such a duty already exists in tort law, but it's inconsistent and often ineffective as applied to digital

---

[121] Hartzog & Richards, *Data Loyalty*, *supra* note 74, at 359.
[122] *Id*.
[123] *Id.* at 370-71; Neil Richards, Woodrow Hartzog & Jordan Francis, *A Concrete Proposal for Data Loyalty*, 37 HARV. J.L. & TECH. 1335, 1345 (2023).

technologies.[124] Lawmakers could also embolden the Federal Trade Commission's prohibition on unfair trade practices to properly respond to the dangers of AI systems, including wrongful discrimination, emotional suffering, financial loss, labor exploitation, and physical harm.[125] This is on top of the need to embolden the technology-agnostic duties already present in civil rights law, employment law, health law, and other contexts in which AI systems are deployed.

2. Design

Companies are often quick to tell you their AI tools are "neutral."[126] They claim that AI is just a tool that can be used for good or bad ends. The argument that flows from the idea of technology as a neutral tool is that lawmakers should regulate not the tool itself but rather the use of that tool.

---

[124] *See generally* Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference*, 69 DUKE L.J. 583 (2019) (detailing the hurdles for plaintiffs bringing products liability and negligence claims because traditional tort law is ill-suited to address modern, Internet-based harms).

[125] *See, e.g.*, Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785 (2015); Andrew D. Selbst & Solon Borocas, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law*, 171 U. PA. L. REV. 1023 (2023).

[126] Cecilia Kang, *OpenAI's Sam Altman Urges A.I. Regulation in Senate Hearing*, N.Y. TIMES (May 16, 2023), https://www.nytimes.com/2023/05/16/technology/openai-altman-artificial-intelligence-regulation.html [https://perma.cc/H3PT-ARX5] ("Ms. Montgomery of IBM called for an A.I. law that is similar to Europe's proposed regulations, which outlines various levels of risk. She called for rules that focus on specific uses, not regulating the technology itself. 'At its core, A.I. is just a tool, and tools can serve different purposes,' she said, adding that Congress should take a 'precision regulation approach to A.I.'"); Richard Socher, *AI Isn't Dangerous, but Human Bias Is*, WORLD ECON. F. (Jan. 17, 2019), https://www.weforum.org/agenda/2019/01/ai-isn-t-dangerous-but-human-bias-is [https://perma.cc/SWZ8-8YVS]; Charles Arthur, *DeepMind: 'Artificial Intelligence Is a Tool That Humans Can Control and Direct'*, GUARDIAN (June 9, 2015, 6:29 AM EDT), https://www.theguardian.com/technology/2015/jun/09/deepmind-artificial-intelligence-tool-humans-control [https://perma.cc/2EFN-M327].

The idea that AI systems are amoral is misguided. There is no such thing as a neutral technology.[127] The purpose of a technology is to create something that will act upon the world, and every design decision makes a certain reality more or less likely. Design choices can accomplish two things: sending signals or making tasks easier or harder. Every design choice is made in furtherance of one or both goals, and the result is always to affect our world. In this sense, design is both power and political, as it affects how power is created, distributed, and used. To pretend that AI is somehow neutral, even the multi-purpose large foundation models, is to allow companies to launder their moral choices that affect billions of people into machines and avoid responsibility for the reality they helped bring about.

This means lawmakers must create design rules for AI. These rules can take several forms, such as secondary liability for product design and requirements and limitations for specific deployments. One great start would be to embolden the FTC's "means and instrumentalities" theory of unfair and deceptive conduct by companies.[128] Under this theory, companies that design AI tools that facilitate unfair and deceptive practices can also be held liable for violating the FTC Act.[129] Lawmakers could expand rules against "abusive" trade

---

[127] *See generally* HARTZOG, *supra* note 5; Langdon Winner, *Do Artifacts Have Politics?*, 109 DAEDALUS 121 (1980); Calo, *supra* note 67; Bruno Latour, *Morality and Technology: The End of the Means*, 19 THEORY CULTURE & SOC'Y 247 (2002); DON NORMAN, THE DESIGN OF EVERYDAY THINGS (rev. ed. 2013); BATYA FRIEDMAN & DAVID G. HENDRY, VALUE SENSITIVE DESIGN: SHAPING TECHNOLOGY WITH MORAL IMAGINATION (2019).

[128] *See, e.g.*, Hartzog, *supra* note 125, at 818-22; Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 663-66 (2014); Andrew Smith, *Multi-Party Liability*, FED. TRADE COMM'N: BUS. BLOG (Jan. 29, 2021), https://www.ftc.gov/business-guidance/blog/2021/01/multi-party-liability [https://perma.cc/R8XP-NECZ].

[129] *See* Complaint ¶¶ 65-66, X-Mode Social, Inc., File No. 212-3038, FTC (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf [https://perma.cc/N97J-LQU4] (alleging that respondent companies "provided the means and instrumentalities for the commission

practices that exploit people's vulnerabilities to confront AI systems that manipulate people into bad choices (also called "dark patterns").[130] Finally, lawmakers should also revitalize

---

of deceptive acts and practices" by "furnish[ing] third party app publishers with language for consumer disclosures in both apps and privacy policies that misleads consumers about the purposes for which their location may be used, such as by failing to disclose that consumer's location would be provided to government contractors for national security purposes"); Lina M. Khan, *Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter and Commissioner Alvaro M. Bedoya Regarding the Final Rule on the Trade Regulation Rule on Impersonation of Government and Business Commission File No. R207000*, FED. TRADE COMM'N 2 (Feb. 15, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/r207000impersonationrulelmkstmt.pdf [https://perma.cc/2666-A5UQ] ("[T]he supplemental proposal also recommends extending liability to any actor that provides the 'means and instrumentalities' to commit an impersonation scam. Under this approach, liability would apply, for example, to a developer who knew or should have known that their AI software tool designed to generate deepfakes of IRS officials would be used by scammers to deceive people about whether they paid their taxes. Ensuring that the upstream actors best positioned to halt unlawful use of their tools are not shielded from liability will help align responsibility with capability and control."); FEDERAL TRADE COMMISSION, SOCIAL MEDIA BOTS AND DECEPTIVE ADVERTISING 4-5 (2019), https://www.ftc.gov/system/files/documents/reports/social-media-bots-advertising-ftc-report-congress/socialmediabotsreport.pdf [https://perma.cc/YG6K-S82Q] (asserting that a provider of AI bots furnished the "means and instrumentalities" of deceptive conduct).

[130] *See, e.g.*, Richards & Hartzog, *supra* note 117, at 1501-02. The Consumer Financial Protection Bureau can regulate "abusive" conduct as well as "unfair" conduct. 12 U.S.C. § 5531(a). An "abusive" practice is one that:

> (1) Materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or (2) Takes unreasonable advantage of:
>
> - A lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service;
> - The inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or
> - The reasonable reliance by the consumer on a covered person to act in the interests of the consumer.

products liability law to better respond to harmful technologies.[131]

Another way lawmakers can take design seriously is to focus on systems and infrastructure.[132] Julie Cohen, for example, argues that treating digital tools more seriously as infrastructure—the structured arrangements that facilitate human activity across space—can help address some of the pathologies plaguing the public sphere. As with digital tools, the function of infrastructure follows its form.[133] Cohen notes that, in many ways, infrastructure thinking is related to but goes beyond the common discourse around "design" because it "probes downward and outward to consider the underlying, habituated arrangements through which activities of exchange and the social orderings they produce are enabled and shaped at scale."[134]

According to Cohen, "[t]he quest for fair choice architectures has a way of rendering underlying arrangements for data harvesting and real-time, data-driven patterning invisible; infrastructure thinking aims to expose those arrangements and consider what they ask us to take for

---

Policy Statement on Abusive Acts or Practices, CONSUMER FIN. PROT. BUREAU (Apr. 3, 2023), https://www.consumerfinance.gov/compliance/supervisory-guidance/policy-statement-on-abusiveness [https://perma.cc/QW5G-EERJ].

[131] *See generally* Crootof, *supra* note 124; Jane Bambauer, *Negligent AI Speech: Some Thoughts About Duty*, 3 J. FREE SPEECH L. 343 (2023); Nina Brown, *Bots Behaving Badly: A Products Liability Approach to Chatbot-Generated Defamation*, 3 J. FREE SPEECH L. 389 (2023); *see also* Complaint for Injunctive and Other Relief, Arizona v. Meta Platforms, Inc., No. 23-CV-05448 (N.D. Cal. Oct. 24, 2023); Complaint for Personal Injuries, C.U. v. Meta Platforms, Inc., No. CGC-22-602249 (Cal. Super. Ct. Oct. 6, 2022).

[132] *See generally* BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES (2012).

[133] Julie Cohen, *Infrastructuring the Digital Public Sphere*, 25 YALE J.L. & TECH. SPECIAL ISSUE 1, 15 (2023) ("Despite—and sometimes because of—their transparency when working as expected, infrastructures do not simply facilitate individual and social activities but also shape them by virtue of the affordances and constraints that they incorporate and continually reinscribe.").

[134] *Id.* at 16-17.

granted."[135] Two areas that Cohen argues deserve more legal scrutiny as a way for platforms to achieve infrastructural scale are algorithmic optimization and platform software development kits (SDKs). Both concepts are also central to deployments of AI and should similarly be the focus of design rules and scrutiny.

3. Defaults

Never underestimate the power of transaction costs and inertia.[136] Mireille Hildebrandt wrote, "We are on the verge of shifting from *using technologies* to *interacting with them*, negotiating their defaults, pre-empting their intent while they do the same to us."[137] Ian Kerr said of Hildebrandt's observation: "Before we had sophisticated machines, it used to be that only nature or humans could be the exclusive architects of our default settings. Now, the defaults settings of the onli*f*e will be negotiated with and by machines without our intervention or oversight. To me, this is a *tectonic shift*."[138] Kerr identified four different kinds of shifting defaults due to digital technologies: (1) natural defaults (such as the natural state of privacy as obscurity), (2) technological defaults (such as the position of switches on privacy dashboards or the design of webpages themselves), (3) legal defaults (such as prohibitions on discrimination or presumptions of authorization to move about in public spaces), and (4) normative defaults (collective presumptions about behavior).[139] These four kinds of defaults often influence each other, such as how technological and legal defaults can shape normative defaults. All four significantly affect our well-being.

Because industry will leverage all four defaults in self-dealing ways, lawmakers must take them all seriously. Kerr,

---

[135] *Id.* at 17.

[136] *See, e.g.*, Hartzog & Selinger, *Loss of Obscurity*, *supra* note 31, at 1355-69; Hartzog & Selinger, *Costs of Harassment*, *supra* note 31, at 48-49.

[137] MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW ix (2015).

[138] Ian Kerr, *The Devil Is in the Defaults*, 4 CRITICAL ANALYSIS L. 91, 94 (2017). Hildebrandt defines the "onli*f*e" as "a transformative life world, situated beyond the increasingly artificial distinction between online and offline." HILDEBRANDT, *supra* note 137, at 8.

[139] *See* Kerr, *supra* note 138, at 91-98.

Hildebrandt, Cohen, and others have wrestled with deep, foundational questions about the ability of AI to restructure law and life.[140] But even in the short term, defaults should be a key aspect for lawmakers regulating AI and its effects. Lawmakers might consider borrowing a few defaults from the European Union's General Data Protection Regulation, such as the presumption that all data processing is prohibited unless affirmatively justified with a legal basis, and the technological rule of "[d]ata protection by design and by default."[141] While there's good reason to think that technological defaults such as "do not track" are slippery and often reinforce the failed "control" paradigm, they can—if structured to advance collective well-being and to protect people no matter what they choose—complement more robust duties and bright-line rules.[142] Lawmakers might also consider frameworks furthering what Danielle Citron has called "technological due process," which include default requirements for meaningful audit trails and opportunities for those affected by AI to challenge decisions made about them.[143]

Some of the most robust defaults lawmakers should consider are presumptive prohibitions absent justifications and demonstrably safe use. These could take the form of licensing regimes, pre-clearance regimes, and other legal frameworks deployed in contexts like healthcare devices and pharmaceuticals.[144] Gianclaudio Malgieri and Frank Pasquale

---

[140] *See generally* HILDEBRANDT, *supra* note 137; Kerr, *supra* note 138; COHEN, *supra* note 6.

[141] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, arts. 6, 25, 2016 O.J. (L 119) 36-37, 48.

[142] *See generally* Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, 80 U. CHI. L. REV. 1155 (2013); Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L.J. 61 (2014).

[143] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1258, 1305-08 (2008).

[144] ACCOUNTABLE TECH, AI NOW INST. & ELEC. PRIV. INFO. CTR., ZERO TRUST AI GOVERNANCE 5-7 (2023), https://accountabletech.org/wp-content/uploads/Zero-Trust-AI-Governance.pdf [https://perma.cc/XF25-286X]; *see also id.* at 2 ("At each phase of the AI system lifecycle, the burden should be on *companies* to prove their systems are *not* harmful.").

have proposed a system of "unlawfulness by default" for AI systems, which would be "an ex-ante model where some AI developers have the burden of proof to demonstrate that their technology is not discriminatory, not manipulative, not unfair, not inaccurate, and not illegitimate in its legal bases and purposes."[145] Licensing as a default for some AI systems would not solve all the problems of AI and would come with its own costs, but it would be one of the most significant steps that lawmakers could take to recognize AI's dangerous affordances.

4. Data Dead Ends

The default position of lawmakers is to assume that all technology is desirable and to go straight to guardrails and procedural rules. It shouldn't be. It's dangerous for lawmakers simply to assume the virtues of astonishingly powerful AI systems. In fact, Evan Selinger and I have argued that some AI systems, such as face surveillance technologies, are too dangerous ever to be safely deployed.[146] When lawmakers go straight to fair-use frameworks, they fail to ask the existential question about whether a particular AI system should exist at all.

But AI systems should not be treated as preordained. They are intentionally designed and built by people, and people can prohibit them, regulate them, and shape their evolution into socially beneficial tools as well. Otherwise, AI tools and information practices should be outright prohibited, what I refer to colloquially as a "dead end." Lawmakers will make little progress until they accept that the toothpaste is never out

---

[145] Gianclaudio Malgieri & Frank Pasquale, *From Transparency to Justification: Toward* Ex Ante *Accountability for AI* 1 (Brook. L. Sch. Legal Stud. Working Paper No. 712, Brussels Privacy Hub, Working Paper No. 33, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4099657 [https://perma.cc/FU84-5XUS]; *see also* Gianclaudio Malgieri & Frank Pasquale, *Licensing High-Risk Artificial Intelligence: Toward Ex Ante Justification for a Disruptive Technology*, 52 COMP. L. & SEC. REV., Apr. 2024, at 1, 15.

[146] *See* Evan Selinger & Woodrow Hartzog, *What Happens When Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html [https://perma.cc/5V93-32ND]; Selinger & Hartzog, *supra* note 7.

of the tube when it comes to questioning and curtailing the design and deployment of AI systems for society's betterment.[147]

In their proposal for "Zero Trust AI Governance," non-profit groups Accountable Tech, the AI Now Institute, and the Electronic Privacy Information Center argued that

> [c]ertain uses of AI are fundamentally incompatible with human rights and should never be permitted, including:
>
> a. Emotion recognition or use of biometrics to infer psychological states
> b. Predictive policing
> c. Remote biometric identification including use of facial recognition in public spaces
> d. Social scoring
> e. Fully automated hiring, firing, and management of workers (including workers classified as independent contractors)[.][148]

I agree.[149] Given industry's extraction, normalization, and exploitative self-dealing inevitabilities, there is no world in which humanity will be better off with these tools. On balance, they will be used as engines for human suffering.

Privacy is the most direct and necessary place to start with AI prohibitions. The root cause of so many problems with AI (and digital technologies generally) is the rot from surveillance-based business models.[150] So, as digital rights organizations, including the Electronic Frontier Foundation, have suggested, it makes sense for lawmakers to start with

---

[147] KAK & WEST, *supra* note 6, at 4 ("[T]here is nothing about artificial intelligence that is inevitable. Only once we stop seeing AI as synonymous with progress can we establish popular control over the trajectory of these technologies and meaningfully confront their serious social, economic, and political impacts . . . .").

[148] ACCOUNTABLE TECH ET AL., *supra* note 144, at 4.

[149] *See* Selinger & Hartzog, *supra* note 7.

[150] *See* COHEN, *supra* note 6, at 25-37; ZUBOFF, *supra* note 20, at 14-16.

privacy as a regulatory strategy.[151] This means lawmakers should create prohibitions on data collection, use, and sharing, both at the point of collection and downstream.

The best way to start holding AI companies accountable is by limiting data collection. That means creating robust data minimization rules to restrict what companies collect and how they can use it.[152] Part of this push should include prohibitions on the collection and use of all sensitive data beyond what is strictly necessary to provide or maintain a specific product or service requested by that individual. Lawmakers should also pass prohibitions on biometric surveillance in education, workplaces, housing, and hiring. To reduce financial incentives to track people's conduct online, lawmakers should prohibit cross-context behavioral advertising.[153] Finally, lawmakers should also consider more ex post prohibitions on data processing as a response to wrongful collection—what Danielle Citron has called "the data death penalty."[154]

Prohibitions are indispensable tools to respond to all three of the dangerous inevitabilities of AI. They outright prevent extraction and deny industry the tools of exploitation at scale. They provide a substantive backstop to prevent the normalization of behavior because they are generally proactive and do not rely upon constantly eroding social norms or people's expectations. Outright prohibitions on collection and

---

[151] Corynne McSherry et al., *To Address Online Harms, We Must Consider Privacy First*, ELEC. FRONTIER FOUND. (Nov. 14, 2023), https://www.eff.org/deeplinks/2023/11/address-online-harms-we-must-first-do-privacy [https://perma.cc/SX77-PYLC] ("A strong comprehensive data privacy law promotes privacy, free expression, and security. It can also help protect children, support journalism, protect access to health care, foster digital justice, limit private data collection to train generative AI, limit foreign government surveillance, and strengthen competition.").

[152] ACCOUNTABLE TECH ET AL., *supra* note 144, at 4 ("Strong data minimization rules . . . represent one of the most powerful tools for addressing the toxic dynamics of the AI arms race—from both a privacy perspective and a competition perspective, as Big Tech's dominance in the space is owed largely to their massive data advantages.").

[153] *Id.*

[154] Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1826-29 (2021); DANIELLE CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE 163-64 (2022).

use are the best way to avoid normative drift and desensitization.

Conclusion

This Essay may strike some as harsh or imbalanced. I have levied critiques of dangerous extraction, harmful normalization, and adversarial self-dealing without focusing much on the potential benefits of AI systems. I am hopeful that AI systems will be developed to allow governments and people to save our planet, keep us healthy, and realize a more just and equitable society than would have been possible otherwise. If lawmakers can advance these goals and not inhibit them, they should. But AI has enough boosters. My point in this critical intervention is that unless a few key dynamics are addressed, AI systems will likely be used in the long run to do more harm than good.

There's much we don't know about how AI systems will work to change our world. But there are a few things that lawmakers should count on. Companies will take everything they can for their own benefit, and we will get used it. People can benefit from AI systems and still be individually and collectively worse off overall. And unless lawmakers create rules to respond to extraction, normalization, and self-dealing, companies will use AI systems to permanently impoverish our lives.