2024

Kafka in the Age of AI and the Futility of Privacy as Control

Daniel Solove

Woodrow Hartzog

KAFKA IN THE AGE OF AI AND THE FUTILITY OF PRIVACY AS CONTROL

BY DANIEL J. SOLOVE* & WOODROW HARTZOG**

ABSTRACT

Despite writing more than a century ago, Franz Kafka captured the core problem of digital technologies—how individuals are rendered powerless and vulnerable. Over the past fifty years, and especially in the twenty-first century, privacy laws have been sprouting up around the world. These laws are often based heavily on an Individual Control Model that aims to empower individuals with rights to help them control the collection, use, and disclosure of their data.

In this Article, we argue that although Kafka starkly shows us the plight of the disempowered individual, his work also paradoxically suggests that empowering the individual isn't the answer to protecting privacy, especially in the age of Artificial Intelligence ("AI"). In Kafka's world, characters readily submit to authority, even when they aren't forced and even when doing so leads to injury or death. The victims are blamed, and they even blame themselves.

Although Kafka's view of human nature is exaggerated for darkly comedic effect, it nevertheless captures many truths that privacy law must reckon with. Even if dark patterns and dirty manipulative practices are cleaned up, people will still make bad decisions about privacy. Despite warnings, people will embrace the technologies that hurt them. When given control over their data, people will give it right back. And when people's data is used in unexpected and harmful ways, they will often blame themselves.

Kafka's writing provides key insights for regulating privacy in the age of AI. The law can't empower individuals when it is the system that renders them powerless. Ultimately, privacy law's primary goal should not be to give individuals control over their data. Instead, the law should focus on ensuring a societal structure that brings the collection, use, and disclosure of personal data under control.

* Eugene L. and Barbara A. Bernard Professor of Intellectual Property and Technology Law, The George Washington University Law School.

** Professor of Law, Boston University School of Law. The authors would like to thank Keenan Hunt-Stone, Caroline Grady, Jeremy Brunner, and the rest of the members of the *Boston University Law Review* for their excellent work on this essay and the entire symposium "Information Privacy Law at the Crossroads."

CONTENTS

INTRODUCTION

At the turn of the twenty-first century, one of us noted that Franz Kafka's *The Trial* was a fitting metaphor for the privacy problems caused by the aggregation of personal data in large computer databases.[1] *The Trial* opens with two officials informing the protagonist, Josef K., that he is under arrest.[2] They don't tell him why—they actually don't know the reason—but they explain that a bizarre clandestine court system has a dossier about him and is making decisions about him. K. desperately—even obsessively—tries to find out more, but he barely learns anything. As one of us wrote, Kafka depicts a "thoughtless process of bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of their information."[3]

We are now nearly a quarter of the way into the twenty-first century, and digital technologies have continued their relentless progression. Organizations are gathering vastly more personal data and are using it to influence and manipulate our behavior. Powerful machine learning algorithmic systems, colloquially known as "Artificial Intelligence" or "AI," are being used to make an ever-expanding range of decisions affecting our lives.

To address these problems, privacy laws have been enacted at a furious pace. By the early 2000s, lawmakers began to realize the need for new surveillance and data protection rules. New laws have sprouted up around the world. The crown jewel of data privacy laws, the European Union's General Data Protection Regulation ("GDPR"), was enacted in 2016.[4] Privacy laws are popping up at the state level in the United States like popcorn kernels in a sizzling frying pan.[5]

Most privacy laws have tried to address the problems that Kafka captured so vividly in his work—the devastating powerlessness of individuals. By and large, most privacy laws have adopted what we refer to as the "Individual Control Model," which seeks to empower individuals to control their data.[6]

In this Article, which serves as an introduction to a symposium on privacy law's past, present, and future, we argue that the Individual Control Model has

[1] *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1398 (2001) [hereinafter Solove, *Privacy and Power*]; DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 36 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON].

[2] FRANZ KAFKA, THE TRIAL 3-19 (Breon Mitchell trans., Schocken Books 1998) (1925).

[3] Solove, *Privacy and Power*, *supra* note 1, at 1398.

[4] *See generally* Regulation (EU) 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[5] *See, e.g.*, VA. CODE ANN. §§ 59.1-575 to 59.1-585 (West 2023); COLO. REV. STAT.§§ 6-1-1303 to 6-1-1313 (West 2024); UTAH CODE ANN.§§ 13-61-101 to 13-61-404 (West 2023); WASH. REV. CODE §§ 19.373.005 to 19.373.900 (West 2023); 2023 Conn. Pub. Acts No. 22-15 (Reg. Sess.).

[6] *See infra* Section I.A.

not only failed, but it is doomed, especially in the age of AI. Intuitively, the Individual Control Model appears to address the problem of individual powerlessness so chillingly portrayed by Kafka. Was it wrong for the law to focus on this problem? We contend that although individual powerlessness is the right problem, the Individual Control Model is the wrong approach to address it.

Revisiting Kafka's work shows us why. A closer look at Kafka's depiction of the individual powerlessness problem reveals its full paradoxical nature. Although individuals are disempowered, the answer isn't to try to empower them with control over their data. In Kafka's fiction, characters readily submit to authority, even when they aren't forced, and even when doing so leads to injury or death. The victims are blamed, and they even blame themselves. In its dark and dramatic way, Kafka's work teaches us that trying to give people control doesn't empower them, and it can even make the situation worse.

Drawing upon Kafka's view of human nature, we argue that the control privacy law gives to people is often turned against them, and that people readily surrender any control they might be given. People eagerly embrace the technologies that hurt them and make choices to their detriment. Although the law should certainly stop organizations from exploiting and manipulating people, merely curtailing these practices isn't enough.

In contrast to the Individual Control Model, we contend that another model would be far more effective—the "Societal Structure Model."[7] This model, which we and other academics have advanced in varying forms and names for many decades, has unfortunately been overlooked by policymakers in their futile quest to make the Individual Control Model work. Instead of trying to empower individuals to control their data, the Societal Structure Model focuses on controlling the power of organizations to collect, use, and disclose personal data and preventing harm to individuals and society.

In Part I we discuss the Individual Control Model and the Societal Structure Model. In Part II, we argue that Kafka's work provides provocative insights into why the Individual Control Model is doomed. In Part III, we contend that the rise of AI makes the futility of the Individual Control Model vividly apparent.

I. TWO MODELS FOR PRIVACY PROTECTION

When the current approach to privacy regulation was being forged during the latter half of the twentieth century, a clash arose between two differing visions of how privacy should be regulated—the Individual Control Model and the Societal Structure Model.

Although many academic commentators recommended the Societal Structure Model, policymakers embraced the Individual Control Model. As is becoming increasingly clear in today's age of AI, the Individual Control Model is the wrong choice.

[7] *See infra* Section I.B.

A. *The Individual Control Model*

The Individual Control Model aims to empower individuals and give them control over their personal data.[8] Professor Alan Westin, perhaps the most influential architect of this approach, proclaimed that privacy was "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[9] The Individual Control Model was embraced in the influential 1973 report by the U.S. Department of Health, Education, and Welfare, which proclaimed that individuals should have "a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it."[10]

Privacy and data protection laws sprouted up in the United States, Europe, and around the world, and most embraced the Individual Control Model in significant part. These laws relied heavily on providing individual privacy rights so that people could manage their data.[11] In the United States, these rights generally included a right to information about data collected about a person, a right to access that data, and a right to correct errors or omissions in the data.[12] European laws provided additional rights such as a right to delete (or erase) data from records, a right to object to the processing of data, a right to not be subject to automated decisions, and more.[13]

In the United States, many laws sought to implement the Individual Control Model through the notice-and-choice approach, where organizations posted notices about their privacy practices and individuals could opt out if they

[8] *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1266 (1998) ("[C]ontrol is at the heart of information privacy."). *See generally* Michael D. Birnhack, *A Quest for a Theory of Privacy: Context and Control*, 51 JURIMETRICS 447 (2011) (reviewing HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010)) (lauding Nissenbaum's theory of privacy centered around control); Michael Birnhack, In Defense of Privacy-As-Control (Properly Understood) (unpublished manuscript) (on file with authors) (defending "privacy as control" model).

[9] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

[10] SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 40-41 (1973).

[11] Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 977 (2023) [hereinafter Solove, *Limitations of Privacy Rights*] ("Privacy laws were developed with the aim of putting individuals back in control of their personal data—and providing for individual rights was an essential way to do so.").

[12] *See, e.g.*, CAL. BUS. & PROF. CODE § 22575(b)(1) (West 2023) (right to information); 15 U.S.C. § 1681g(a) (right to access); VA. CODE. ANN. § 59.1-577(A)(3) (West 2023) (right to correct errors or omissions).

[13] *See, e.g.*, GDPR, *supra* note 4, at arts. 17, 21, 22.

objected.[14] Of course, people don't read privacy notices and have no clue what is being done with their data. Nobody really took notice-and-choice seriously; it has been thoroughly and continually skewered by commentators.[15]

Another hallmark of the Individual Control model involves consent requirements.[16] In the European Union's data protection approach, consent must be express and affirmative (opt-in).[17] Although express consent is far superior to the notice-and-choice approach, it still depends heavily on the ability of individuals to make meaningful decisions about the collection and use of their data. Regardless of whether consent requirements are strict or lax, opt-in or opt-out, consent is, at its core, about individual control.

B. *The Societal Structure Model*

In contrast to the Individual Control Model, leading scholars have long advocated for the Societal Structure Model. This view begins with the recognition that privacy is not purely (or even primarily) an individual interest; instead, privacy should be protected for the purpose of promoting societal values such as democracy, freedom, creativity, health, and intellectual and emotional flourishing.[18] Many scholars, especially Paul Schwartz, Oscar Gandy, Julie Cohen, Joel Reidenberg, Spiros Simitis, and Priscilla Regan, have long pointed out the importance of viewing privacy as a societal value, not just an individual interest.[19]

---

[14] *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS i-iii (2010) (recognizing Federal Trade Commission used notice-and-choice model to encourage companies to develop notices describing information collection to consumers).

[15] *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1704 (2020) ("'[N]otice' often means little more than burying data practices in the fine print of a dense privacy policy, while 'choice' means choosing to use a service with its non-negotiable data practices as a take-it-or-leave-it option.").

[16] Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 604 ("Many privacy laws rely heavily on consent as a means to legitimize data collection and processing because consent carries such significant 'moral force.'"); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1476-91 (2019) (detailing three "Pathologies of Consent," which describe defects consent suffers: unwitting consent, coerced consent, and incapacitated consent).

[17] *See* Solove, *Limitations of Privacy Rights*, *supra* note 11, at 982-83 (discussing comprehensive set of rights detailed in GDPR).

[18] *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1647-58 (1999) (discussing lack of privacy as hindrance on capacity for self-governance and participation in American deliberative democracy); Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 866 (2000) (arguing American right to privacy should stem from American ideal to be free from "unwanted intervention, decisional autonomy, and freedom of choice generally").

[19] *See generally* OSCAR H. GANDY JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (2d ed. 2021) (noting dangers of information access in exacerbating existing societal inequities); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY,

Under this view, privacy is first and foremost about power and how human information is relevant in its creation, deployment, and distribution.[20]

We both joined the Societal Structure Party in the early twenty-first century. As Solove contended, "the protection of privacy depends upon an architecture that structures power, a regulatory framework that governs how information is disseminated, collected, and networked. We need to focus on controlling power."[21] Hartzog rejected the Individual Control Model as illusory, overwhelming, and myopic, advocating for design rules and a better structural allocation of power instead.[22]

As the twenty-first century unfolded, many scholars joined in to advocate for the Societal Structure Model.[23] We and many others have fleshed out the contours of structural approaches for protecting trust within information

SOCIAL VALUES, AND PUBLIC POLICY 225 (1995) (describing importance and difficulties in legislating privacy as societal value); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709 (1987) ("[P]rivacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone."); Schwartz, *supra* note 18 (critiquing the "autonomy trap"); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) [hereinafter Cohen, *Examined Lives*] (arguing individual autonomy relies on freedom from monitoring and scrutiny of others); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 882-83 (2002) ("Society as a whole has an important stake in the contours of the protection of personal information."); Allen, *supra* note 18 (articulating conceptual, practical, and moral limits of privacy-control paradigm).

[20] *See* Cohen, *Examined Lives*, *supra* note 19, at 1377-91 (discussing privacy as it relates to property and ownership power).

[21] SOLOVE, THE DIGITAL PERSON, *supra* note 1, at 101.

[22] *See generally* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018); Woodrow Hartzog, Opinion, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423 (2018).

[23] *See, e.g.*, Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIA. L. REV. 559, 563 (2015) ("[F]ree choice is not the shibboleth of privacy in the information-sharing context."); Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 462 (2020) ("[The paradigm] must shift from a liberalist regulatory approach that seeks to facilitate individual choice, to one that empowers public officials to make choices about which . . . practices are safe for individuals and consistent with social values and which are not.").

relationships,[24] for a relational approach to data governance,[25] for the natural obscurity that people create and rely upon for their everyday lives,[26] for the contextual integrity of personal information flows,[27] for privacy as a public good,[28] and for nonwaivable privacy entitlements,[29] among other concepts that extend beyond notions of individual control.

[24] Early proponents of this theory include Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419, 446-47 (2001), and SOLOVE, THE DIGITAL PERSON, *supra* note 1, at 102-04. Later on, Neil Richards and Woodrow Hartzog wrote extensively about trust and the duty of loyalty. *See generally* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*]; Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180 (2017); Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 6 EUR. DATA PROT. L. REV. 492 (2020); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021) [hereinafter Richards & Hartzog, *Duty of Loyalty*]; Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985 (2022); Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356 (2022). Other notable scholarship on relationships and trust includes Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016) [hereinafter Balkin, *Information Fiduciaries*], ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 8 (2018), Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1058 (2019), Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 11 (2020) [hereinafter Balkin, *Fiduciary Model of Privacy*], Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 144-45 (2020), and Claudia Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34, 35 (2020).

[25] Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 578 (2021) ("If data-governance law is inattentive to how data production creates social benefits and harms, it will be poorly equipped to mitigate those harms and foster data production's benefits.").

[26] *See* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1345-46 (2015) (explaining significance of obscurity in modern debates about government surveillance); Woodrow Hartzog & Evan Selinger, *Increasing the Transaction Costs of Harassment*, 95 B.U. L. REV. ANNEX 47, 47-52 (2015) (analyzing industry efforts to mitigate online harassment); Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* SPACES FOR THE FUTURE: A COMPANION TO PHILOSOPHY OF TECHNOLOGY 119, 120-22 (Joseph C. Pitt & Ashley Shew eds., 2018) (arguing information is safe in state of obscurity because it is hard to obtain or understand); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 5 (2013) (explaining obscurity of individual protects them from identification and facilitates social interaction); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 385 (2013) ("Obscurity is the optimal protection for most online social interactions . . . .").

[27] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 14 (2010) (analyzing contextual integrity as degree to which people's expectations for safeguarding of personal information in any given context are met).

[28] *See* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 386 (2015) (asserting that privacy has aspects of public good, which makes it good candidate for group coordination).

[29] *See* ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 8 (2011).

As Professor Julie Cohen has expressed so aptly: "[P]rivacy incursions harm individuals, but not only individuals. Privacy incursions in the name of progress, innovation, and ordered liberty jeopardize the continuing vitality of the political and intellectual culture that we say we value. A structural understanding of privacy's importance demands a structural approach to privacy regulation."[30]

C. *The Dominance of the Individual Control Model*

Ultimately, the commentators advocating for the Societal Structure Model did not convince lawmakers to implement their proposals and resigned themselves to write in dissent of existing and proposed privacy laws. Policymakers powered forward with the goal of arming individuals with rights.

In 2016, the European Union enacted the GDPR.[31] The GDPR, however, still has informational self-determination as its beating heart. Although it has many provisions that draw from the Societal Structure Model (requirements to justify data processing, minimize data collection and use, data protection impact assessments, data protection by design and default, vendor management, etc.), the GDPR still rests heavily on individual control.[32] The GDPR allows a wide range of data processing with consent.[33] GDPR data protection also depends significantly on individual rights, which occupy a substantial amount of internal organizational compliance efforts and external enforcement.[34]

For automated decision making, the GDPR's protections rely prominently on giving individuals a right to have a human involved,[35] even though in many contexts it remains unlikely that placing humans in the loop will improve the decisions.[36] Professors Talia Gillis and Josh Simons aptly critique the GDPR's approach for relying too much on individual control: "Institutions should justify their choices about the design and integration of machine learning models not to individuals, but to empowered regulators or other forms of public oversight bodies."[37]

---

[30] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906 (2013).

[31] *See* GDPR, *supra* note 4.

[32] Solove, *Limitations of Privacy Rights*, *supra* note 11, at 977 (noting GDPR and other privacy laws aim to put "individuals back in control of their personal data").

[33] IGNACIO COFONE, THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY 90 (2023) (noting seventy-two references to consent in GDPR).

[34] Solove, *Limitations of Privacy Rights*, *supra* note 11, at 978 (explaining GDPR protects data by means of eight individual rights).

[35] GDPR, *supra* note 4, at art. 22.

[36] Ben Green, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, COMPUT. L. & SEC. REV., July 2022, at 1, 7 (noting "automated systems may simply lead to different types of errors rather than reducing overall errors" due to "automation bias"); Rebecca Crootof, Margot E. Kaminski & W. Nicholson Price II, *Humans in the Loop*, 76 VAND. L. REV. 429, 468-69 (2023) (discussing over-deference to automated processing leading to "skill fade" in supervising humans).

[37] Talia B. Gillis & Josh Simons, *Explanation < Justification: GDPR and the Perils of Privacy*, 2 PA. J.L. & INNOVATION 71, 81 (2019).

As Professor Margot Kaminski notes, the GDPR, to its credit, "attempts to provide backstops beyond individual control."[38] But these structural elements are not strong enough; too much of the GDPR rests on individual control. Many of these structural elements are rather barebones measures that lack sufficient accountability or scrupulousness. As Professor Ari Waldman contends, compliance measures can become hollow, performative paper-pushing exercises.[39] Many of the GDPR's structural elements lack the same muscle and rigor as the GDPR's individual control elements. For example, requirements to perform privacy-impact assessments and engage in data protection by design and default lack sufficient specificity or accountability, allowing companies to do them in minimalistic and perfunctory ways.[40] And beyond the GDPR, privacy laws around the world rely much more heavily on individual control, especially via individual consent.[41]

Despite being partially influenced by the GDPR, recent U.S. state consumer privacy laws are firmly founded upon the Individual Control Model. Within months of the GDPR going into effect in 2018, California enacted the California Consumer Privacy Act ("CCPA").[42] In the ensuing years, many other states followed suit, enacting similar laws.[43] These laws, however, are still largely layered on the bones of the notice-and-choice model, with a few structural pieces from the GDPR sprinkled in. The laws have ventured a bit beyond Individual Control Model, but not far enough. For example, the CCPA's regulations have echoed some of the structural provisions of the GDPR, but still focus on people's expectations and choices.[44] While the GDPR at least has a notable footing in the Societal Structure Model, the other U.S. state consumer privacy laws have only a toe in it.

Policymakers keep passing privacy laws at a fever pitch, but most of them still cling to the Individual Control Model. There are a few recent exceptions where lawmakers have embraced the Societal Structure Model, such as the

[38] *See* Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1590 (2019) (comparing additional backstops to previous Fair Information Practices that can lack "substance, providing individuals the illusion of control, while in practice allowing companies to do nearly anything as long as they have gotten individuals to click through an agreement").

[39] ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 9-10 (2021).

[40] *See* GDPR, *supra* note 4, at arts. 25, 35.

[41] COFONE, *supra* note 33, at 90 ("The GDPR may be the data protection legislation in the world that places the least weight on consent.").

[42] CAL. CIV. CODE §§ 1798.100 to 1798.199 (West 2024).

[43] *See, e.g.*, VA. CODE ANN. §§ 59.1-575 to 59.1-585 (West 2023); COLO. REV. STAT. §§ 6-1-1303 to 6-1-1313 (West 2024).

[44] *See, e.g.*, CAL. CIV. CODE § 1798.120(a) (providing for right to opt out of data being sold).

European Union's AI Act[45] and the Digital Services Act,[46] which work primarily through substantive rules and duties aimed at limiting risk and harm regardless of an individual's consent or control. But for the most part, privacy law could have been much better prepared for the risks of AI had it been built upon the Societal Structure Model rather than the Individual Control Model.

II. KAFKA AND THE FUTILE QUEST TO EMPOWER INDIVIDUALS

Kafka's works provide vexing and dismaying reasons why the Individual Control Model is doomed. The impetus for the Individual Control Model stems from how radically people are disempowered when their data is being collected, used, and transferred. Kafka's writings adeptly capture people's harrowing helplessness and vulnerability when at the mercy of powerful and opaque entities that have dossiers about them and that make important decisions about their lives. Kafka's characters often suffer at the mercy of impersonal and uncaring bureaucratic processes; people's fates are decided in standardized ways that ignore the whole story and human texture of their lives.

On the surface, the goal of individual control makes sense; people are being disempowered, so the law should try to combat disempowerment with empowerment. If privacy losses are interferences with autonomy, then more control seems like a sensible answer. As privacy problems have grown more dire, policymakers have reacted by giving individuals more rights, more notice, more choices, and more self-management. But as Kafka's work demonstrates, this strategy will fail to meaningfully protect the vulnerable from the powerful.

A. *Kafka's Dark Portrait of Human Nature*

Throughout his work, Kafka paints a dark portrait of human nature. He vividly captures the plight of the weary individual. Officials are whipped for failures they can't control;[47] people are put on trial without being told what they did wrong;[48] a man wakes up transformed into a monstrous insect and is treated with disdain;[49] and countless other people face absurd, unjust, and humiliating circumstances. There are no happy endings; people are never able to extricate themselves from their situations. With Kafka, things start out badly, then they grow worse.

Turning to modern digital technologies, individual control is often an illusion. People don't exercise control in a meaningful way. Merely being in a command

[45] *See infra* notes 108-12 and accompanying text.

[46] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC, 2022 O.J. (L 277) 1.

[47] *See generally* FRANZ KAFKA, IN THE PENAL COLONY (Willa Muir & Edwin Muir trans., 1948) (1919), *reprinted in* THE COMPLETE STORIES 165 (Nahum N. Glatzer ed., 1971) [hereinafter FRANZ KAFKA, IN THE PENAL COLONY].

[48] *See generally* FRANZ KAFKA, THE TRIAL, *supra* note 2.

[49] *See generally* FRANZ KAFKA, THE METAMORPHOSIS (David Wyllie trans., 2009) (1915).

center with various switches, buttons, and levers is mere theater unless people have the ability and knowledge to operate the controls. The individual's ability to exercise control always exists within a larger power structure.

One hope with privacy law is that it can protect people by stopping organizations from coercing, manipulating, and exploiting them. Many privacy laws aim to ensure that organizations are more transparent about data collection and use, to stop dark patterns and other manipulative practices, and to require organizations to give people choices to opt in, opt out, or delete their data.[50]

These protections are good, but Kafka's work teaches us that these measures are far from enough. The most challenging and deeply disturbing dimension to Kafka's depiction of human nature is that people are often not passive victims; they willingly participate in their peril. They rush toward it and embrace it. In some cases, they even crave it. Surveillance isn't just hoisted upon people; many people eagerly sign up for it.[51] People embrace and normalize the fruits of the digital age, no matter how poisonous they might be.[52] People will often make choices that are not in their own best interest.

In her incisive takedown of legal scholar Richard Posner's law and economics work, Professor Robin West compares Kafka's vision of human nature to Posner's "simplistic and false psychological theory of human motivation."[53] Posner's view of human nature is that people enter into transactions "for only one reason—to maximize their own welfare."[54] West argues that "[w]hereas Posner's characters relentlessly pursue autonomy and personal well-being, Kafka's characters just as relentlessly desire, need, and ultimately seek out authority."[55] She notes that Kafka's characters consent to being controlled. People don't "calculate all of the time"—they often "simply obey, acquiesce, or submit."[56]

Kafka's depiction of human nature serves not only as a counterpoint to Posner but also to the Individual Control Model. Kafka shows us that it is profoundly difficult to empower people, not just because the forces arrayed against them are overpowering, but also because people willingly surrender to those forces. For example, in *The Judgment*, when a despicable father chastises his son and tells

[50] *See supra* Section I.A.

[51] Chris Gilliard, *The Rise of 'Luxury Surveillance'*, ATLANTIC (Oct. 18, 2022), https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772/ ("At the end of September, Amazon announced a suite of tech products in its move toward '"ambient intelligence",' which Amazon's hardware chief, Dave Limp, described as technology and devices that slip into the background but are '"always there",' collecting information and taking action against it.").

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

[53] Robin West, *Authority, Autonomy, and Choice: The Role of Consent in the Moral and Political Visions of Franz Kafka and Richard Posner*, 99 HARV. L. REV. 384, 385 (1985).

[54] *Id.* at 387.

[55] *Id.*

[56] *Id.* at 425.

him to drown himself, the son willingly carries out his father's sentence.[57] In the parable, *Before the Law*, which is a part of Kafka's *The Trial*, a man arrives at the gates to the Law and wants to enter, but a doorkeeper recommends that he not do so.[58] Although the doorkeeper does nothing to stop the man from proceeding, the man "decides he would prefer to wait until he receives permission to enter."[59] He waits for years and years, constantly begging to be admitted. Then he dies.[60] And more broadly in *The Trial*, Josef K. believes in the legitimacy of the court system despite countless signs it is illegitimate—the offices are in attics in rundown buildings; court proceedings are held in decrepit living rooms; what appear to be law books are not.[61] At every turn, the system is unprofessional and even ramshackle. Yet, Josef K. accepts its authority and willingly submits to its power—even his own execution.[62] In each piece, people acquiesce to authority without being forced to do so.

Kafka's works defy simple explanations as to why people make these ruinous decisions to submit. Kafka invites us to contemplate the bewildering complexity and absurdity of human psychology with all its restless emotions, sudden impulses, inexplicable irrationality, contradictory dimensions, and subconscious forces. Kafka shows us that we must reckon with this side of human nature.

As with Kafka's characters, in the real world, people frequently make detrimental and submissive privacy decisions.[63] People often trust companies without much basis (and sometimes contrary to the previous actions by these entities).[64] People readily click the "accept" button or share their data without even trying to exercise their choices.[65] For the most part, people just follow along and do what companies want them to do.

In Kafka's writings, people repeatedly take actions that are not only against their own self-interest, but also harmful and destructive to themselves. In *The Hunger Artist*, the protagonist sits in a cage at a carnival and starves himself to death, not because he wants to entertain the public, but because he can't find any food that will satisfy him.[66] Compare this to the paradox of choice that confounds every person confronted with an overwhelming number of options to

[57] FRANZ KAFKA, THE JUDGMENT (Willa Muir & Edwin Muir trans.) (1912), *reprinted in* THE COMPLETE STORIES 101, 113 (Nahum N. Glatzer ed., 1971).

[58] FRANZ KAFKA, THE TRIAL, *supra* note 2, at 218.

[59] *Id.* at 216.

[60] *Id.* at 217.

[61] *Id.* at 65.

[62] *Id.* at 229-30.

[63] *See* Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509, 510 (2015) (explaining even when participants "expressed the highest degree of concern" many of them still revealed personal information online).

[64] *See id.* at 512.

[65] *Id.* at 513.

[66] *See generally* FRANZ KAFKA, THE HUNGER ARTIST (Edwin Muir and Willa Muir trans., 1948) (1922), *reprinted in* THE COMPLETE STORIES 300 (Nahum N. Glatzer ed., 1971).

control their data, none of which quite fit their preferences or the real risk of exposure.[67]

Giving Kafka's characters more control won't save them. They aren't compelled into their fates; they often actively participate in their own demise. For privacy, the same phenomena are occurring. People readily "consent" to the widespread indiscriminate collection and use of their data.[68] Sometimes this is because companies exploit and trick people into submitting.[69] But many times, companies can just nudge, tempt, or seduce people into the behaviors that generate profit, which often involve people maximally exposing their data.[70] Kafka's stories provide the lesson that people might still be disempowered even when companies aren't acting maliciously. When given power, people often will give it right back. If people are given opt-in rights, companies will lure people to opt in. If people are given property rights in their data, companies will entice them to trade those rights for trinkets.

The behavior of Kafka's characters might be a comic exaggeration, but Kafka captures many disturbing truths about human nature, which is why his works have endured and still resonate with readers today. Psychologist Stanley Milgram's studies have shown that people readily submit to authority.[71] People can develop harmful technological dependencies.[72] People often act against their

[67] *See* Laura Brandimarte, Alessandro Acquisti & George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCH. & PERSONALITY SCI. 340, 345 (2012) (demonstrating how technology designed to increase people's control over information leads them to release more information); Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 448-49 (2016) (arguing consumers have asymmetric information on how, when, and why their data is collected, hindering their ability to make informed decisions about privacy); Acquisti et al., *supra* note 63, at 509-14 (summarizing how people's concerns over privacy are context dependent, manipulable, and caused by uncertainty).

[68] *See* Solove, *Murky Consent*, *supra* note 16, at 605-07.

[69] *Id.* at 608-09.

[70] *See* JULIE COHEN, BETWEEN TRUTH AND POWER 71 (2019) ("[T]echniques 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. 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." (footnote omitted)).

[71] *See generally* STANLEY MILGRAM, OBEDIENCE TO AUTHORITY: AN EXPERIMENTAL VIEW (1974) (demonstrating participants' surprising willingness to obey cruel orders).

[72] Doreen Dodgen-Magee, Opinion, *Tech Addiction Is Real. We Psychologists Need To Take It Seriously*, WASH. POST (Mar. 18, 2019, 3:14 PM), https://www.washingtonpost.com/opinions/tech-addiction-is-real-we-psychologists-need-to-take-it-seriously/2019/03/18/5f12ad2e-3c54-11e9-a06c-3ec8ed509d15_story.html.

own self-interests, sometimes in highly self-destructive ways.[73] Not only do people fail to act rationally, but they also act in absurdly unproductive ways.

These dimensions of human nature demonstrate that merely giving people options will not be enough. Nor will it be sufficient to merely hand people power, as they might give it right back.

The Individual Control Model assumes that if people are given the tools to manage their privacy, they will effectively do so, or at least have a meaningful opportunity to try.[74] But the task of privacy self-management is an impossible one—people can't exercise their privacy rights at scale; nor can people learn enough to effectively determine the risks when sharing their data or make appropriate cost-benefit decisions.[75] Kafka also shows us that even if privacy self-management were somehow possible at scale, many people might not behave as the Individual Control Model envisions. Instead, if bestowed with control over their data, people will willingly cede it to the large entities that are collecting and using their data. And they will do so even when it harms them.

B. *Blaming the Victims, Blaming Ourselves*

Kafka's characters internalize the absurd, arbitrary, and unfair forces against them. They feel guilty and fault themselves for being victims. Kafka doesn't explain why people behave in this way; his works starkly illuminate these peculiar phenomena and invite us to ponder why.

In the context of data privacy, people behave in similar ways to Kafka's characters, oddly internalizing the blame when their data is misused. In a study, Professors Yafit Lev-Aretz and Aileen Nielsen found that people often blame themselves when their data is used in unexpected and undesired ways.[76] In Kafkaesque form, people turned inward, faulting themselves. Of course, the system is at fault—it sets people up with the impossible and burdensome task of privacy self-management where failure is a foregone conclusion.[77]

---

[73] *See* Iskra Fileva, *Why We Choose To Act Against Our Own Interests*, PSYCH. TODAY: BLOG (June 15, 2021), https://www.psychologytoday.com/us/blog/the-philosophers-diaries/202106/why-we-choose-act-against-our-own-interests (discussing Freud and Dostoyevsky's understandings of self-destructive tendencies in humans).

[74] *See* Richards & Hartzog, *supra* note 16, at 1461 (explaining failures of consumer consent in context of digital privacy rights).

[75] Solove, *Limitations of Privacy Rights*, *supra* note 11, at 985-87 (explaining that individuals do not have sufficient time or resources to adequately exercise control over their data); HARTZOG, PRIVACY'S BLUEPRINT, *supra* note 22, at 57 ("By ostensibly giving users every conceivable option and every possible relevant piece of information, companies can claim their designs are user- (and privacy-) friendly. . . . Plentiful prestructured choices can overwhelm us or distract us from critically examining the options we *haven't been* given.").

[76] Yafit Lev-Aretz & Aileen Nielsen, Privacy Notice and the Blame Game 5 (2023) (unpublished manuscript) (on file with authors) (explaining role of morality in consumer attitudes toward data-privacy practices).

[77] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883-86 (2013) (explaining cognitive processes that make privacy

This is the situation many organizations desire—it shifts the blame to the victims. Companies can merrily go on doing whatever they please; policymakers can pat themselves on the back for giving consumers rights; and when people fail to use these rights, they can be blamed for not caring enough about their privacy. In what has become known as the "Privacy Paradox," people say they value privacy yet fail to take steps to protect it.[78] Commentators then proclaim that people's behaviors indicate they don't really care about privacy. For example, Professor Omri Ben-Shahar concludes that people barely value privacy protections and are "nonchalant with respect to aggressive collection of their personal information."[79]

In the related context of data security, we have noted that people are routinely expected to perform security best practices despite lacking the capacity to do so.[80] They must memorize long and complex unique passwords for hundreds (sometimes thousands) of accounts; they must become experts in spotting phishing attempts and spoofed emails and websites.[81] People are destined to fail, and when they do, they are chastised for being foolish for choosing bad passwords or falling for phishing tricks.

Instead of empowering people, the law provides the illusion of empowerment while actually further disempowering people, throwing them into a Kafka story of blame, guilt, and impossible endless tasks. The very laws aimed at protecting us are—in perhaps a most fitting Kafkaesque irony—worsening our plight and its utter absurdity.

C. *Surrendering to the Machines: The Technology Trap*

Kafka's story, *In the Penal Colony*, captures our relationship to technology in a shocking and thought-provoking way that has further lessons for privacy law. An officer at a penal colony proudly shows off his elaborate torture and execution machine to an explorer.[82] To the explorer's surprise, the officer suddenly strips off his clothes and climbs into the machine.[83] The machine's gears start turning, beginning the process of etching words on his body with its needles.[84]

self-management difficult); Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551, 568-76 (2023) (describing informational burdens complicating privacy self-management).

[78] Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 2 (2021) ("In surveys, people say that they value privacy highly, yet they readily give away sensitive personal information for small discounts or tiny benefits—or sometimes for nothing at all.").

[79] Omri Ben-Shahar, *Privacy Is the New Money, Thanks to Big Data*, FORBES (Apr. 1, 2016, 3:48 PM), https://www.forbes.com/sites/omribenshahar/2016/04/01/privacy-is-the-new-money-thanks-to-big-data/?.

[80] DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 14 (2022).

[81] *Id.*

[82] FRANZ KAFKA, IN THE PENAL COLONY, *supra* note 47, at 165-67.

[83] *Id.* at 186-88.

[84] *Id.* at 188-89.

But the machine malfunctions, turning the demonstration into a horrific and bloody nightmare.[85]

Just as the officer willingly tries out his own machine, despite the lethal consequences, people are drawn to dangerous technologies. People embrace technology even when it will harm them.[86] Companies offer a cornucopia of exciting and addictive new technologies, from smart phones to home assistant devices to smart doorbells to security cameras to gaming consoles to AI tools to social media and more. When people embrace these dazzling creations, which are designed to extract their data as the price, they are blamed for not caring about their privacy.

People use these technologies despite dire warnings, blinking red lights, and blaring alarms.[87] They install them into their homes, carry them around in their pockets, strap them to their wrists and heads, and put them inside of their bodies. They eagerly plug themselves into the matrix. They are told that the cost for all this must be their privacy, even though nothing makes this tradeoff inevitable.[88] In fact, all the while, people lament the loss of privacy and overwhelmingly say they want more privacy, but they still use privacy-invasive technologies.[89] The law's answer: more transparency. If we just tell people what will be done with their data, if people were better informed, then they would be able to resist all the scrumptious entrees at the technology buffet. Tech evangelists like Nir Eyal advocate that we just reclaim personal responsibility and teach ourselves to resist these temptations.[90] But Kafka shows us that often no amount of education will change people's course. People will still eat the food even if they know it is laced with poison. The food is simply too delicious.

If Kafka were writing about AI, he'd likely not use the typical science fiction plot of robots suddenly desiring to rule us or exterminate us. For Kafka, we'd willingly submit to the robots and beg them to rule us.

---

[85] *Id.* at 190.

[86] *See, e.g.*, GAIA BERNSTEIN, UNWIRED: GAINING CONTROL OVER ADDICTIVE TECHNOLOGIES 16-32 (2023) (discussing widespread adoption of educational video games for children despite evidence of cognitive impairment and addiction).

[87] *See* Dodgen-Magee, *supra* note 72 ("[T]he World Health Organization recognized Internet gaming as a diagnosable addiction.").

[88] *See* Ben-Shahar, *supra* note 79 (noting consumers exchange their privacy for "free" services, such as search engines, they could otherwise afford with traditional currency).

[89] *Id.* ("People do say that they prefer their computer search histories to be discrete, but they are not willing to spend any money [to] do so: only 16% of respondents in another study were willing to spend half-a-penny per search to make it private.").

[90] *See* Nellie Bowles, *Addicted to Screens? That's Really a You Problem*, N.Y. TIMES (Oct. 6, 2019), https://www.nytimes.com/2019/10/06/technology/phone-screen-addiction-tech-nir-eyal.html ("'We talk about addiction, but when it comes to Candy Crush, really? Facebook? We're not freebasing Facebook. We're not injecting Instagram here. . . . These are things we can do something about, but we love to think the technology is doing it to us.'" (quoting Nir Eyal)).

III. PRIVACY, AI, AND SOCIETY

We are now several decades into the twenty-first century, and AI is the rage. But AI is hardly new; in fact, it's quite old. The term "Artificial Intelligence" was coined by computer scientist John McCarthy back in 1955 at Dartmouth.[91] Despite decades of ensuing development and enthusiasm, the results were disappointing.[92] We never saw the rise of robots that could think as science fiction had envisioned (the idea that machines can ever "think" like humans is a dangerous narrative that distracts the discourse about the risks of AI).[93] What we call "Artificial Intelligence" today is just the product of a very effective rebrand of algorithms and data in automated systems that can calculate inferences based on patterns in massive quantities of data.[94] As Professors Chris Wiggins and Matthew Jones aptly observe, "Machine learning, especially machine learning using neural nets, was rebranded as AI by corporate consultants and marketers, sometimes to the discomfort of researchers."[95]

The concepts and concerns with today's AI have been quite similar throughout the years. Commentators in the 1960s and 1970s foresaw how computers would transform the collection of personal data and the way decisions would be made about people.[96] They spoke in terms of "data banks."[97] These concerns grew in the 1980s and 1990s.[98] The rise of the commercial Internet in the late 1990s sparked grave concerns about massive databases about individuals.[99] The term "data banks" had morphed into "databases."[100] One of us called the analysis

[91] CHRIS WIGGINS & MATTHEW L. JONES, HOW DATA HAPPENED: A HISTORY FROM THE AGE OF REASON TO THE AGE OF ALGORITHMS 126-27 (2023) (discussing McCarthy's use of such term to secure funding from Rockefeller Foundation for summer study).

[92] *Id.* at 182 (noting late-1980s "AI winter," a drought of funding for AI projects caused by gaps in theory and practical results).

[93] *Id.* at 183 ("Unlike more ambitious forms of artificial intelligence seeking to emulate *how* humans make decisions, the makers of [machine learning] algorithms viewed them as acting in no way like human brains.").

[94] *Id.* at 190 (characterizing contemporary "redefinition of machine learning as focused on prediction, large data sets, and big computers").

[95] *Id.* at 190-91.

[96] Arthur R. Miller, *Computers, Data Banks, and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1, 2 (1972) (warning large collections of data would be used by employers, insurers, and creditors to discriminate against members of public).

[97] *Id.*

[98] *See, e.g.*, Solove, *Privacy and Power*, *supra* note 1, at 1447 ("In the early 1990s, in response to a public outcry, Lotus Corporation scrapped plans to sell a database containing the names, addresses, income brackets, and lifestyle data of 120 million citizens.").

[99] *See id.* at 1447-48 (recounting public resistance to Lexis-Nexis' and AOL's data collection and Electronic Privacy Information Center's survey of collection practices of websites lacking explicit privacy policies).

[100] *See, e.g.*, ARTHUR M. HUGHES, THE COMPLETE DATABASE MARKETER: SECOND-GENERATION STRATEGIES AND TECHNIQUES FOR TAPPING THE POWER OF YOUR CUSTOMER DATABASE 2 (2d ed. 1996).

of data to make inferences about people the "aggregation effect."[101] The term "data mining" became in-vogue in the early twenty-first century, followed by the uber-popular term "Big Data" to capture large-scale data gathering and analytics. Recently, terms such as "algorithms" and "inferences" are being used with greater frequency, along with the flashier term "Artificial Intelligence," which is used for nearly everything involving algorithms today.[102] But the word "intelligence" is a misnomer—there is still nothing intelligent about Artificial Intelligence.[103]

The rebrand to AI, though, has been quite effective in finally bringing many policymakers and others to realize the shortcomings of the Individual Control Model.[104] AI appears to be endlessly complicated, opaque, inexplicable, and frightening. AI output is produced by determining patterns in massive quantities of data about millions of people.[105] Because decisions based on AI about a person are made based upon data about other people, providing individuals with control over their own data is plainly inapposite. As Professor Alicia Solow-Niederman notes, this type of algorithmic decision "disempowers individuals about whom inferences are made, yet who have no control over the data sources from which the inferential model is generated."[106] Similarly, Professor Salomé Viljoen argues that privacy law's focus on "individualist claims subject to individualist remedies . . . are structurally incapable of representing the interests and effects of data production's population-level aims."[107] The fictions justifying the Individual Control Model have trouble creating any plausible account of how the model is to work for modern AI technologies.

Policymakers finally appear to be losing hope that individuals are able to exercise control over these powerful and bewildering systems. They are enacting and proposing new laws to address AI that go far beyond the Individual Control

---

[101] SOLOVE, THE DIGITAL PERSON, *supra* note 1, at 44 ("Similar to a Seurat painting, where a multitude of dots juxtaposed together form a picture, bits of information when aggregated paint a portrait of a person.").

[102] *See* María P. Angel, *Privacy's Algorithmic Turn*, 30 B.U. J. SCI. & TECH. L. (forthcoming 2024) (manuscript at 18), https://ssrn.com/abstract=4602315 (discussing shift in focus in privacy law scholarship to focus on algorithms).

[103] *See* Hideyuki Matsumi & Daniel J. Solove, *The Prediction Society: AI and the Problems of Forecasting the Future* 5 (George Washington Univ. L. Sch., Pub. L. & Legal Theory Rsch. Paper No. 2023-58, 2023), https://ssrn.com/abstract=4453869 ("[T]he new wave of artificial intelligence does not actually bring us intelligence but instead a critical component of intelligence—*prediction*." (quoting AJAY AGRAWAL, JOSHUA GANS & AVI GOLDFARB, PREDICTION MACHINES: THE SIMPLE ECONOMICS OF ARTIFICIAL INTELLIGENCE 2 (2018)).

[104] *See supra* Section I.A.

[105] *See* Matsumi & Solove, *supra* note 103 (manuscript at 47).

[106] Alicia Solow-Niederman, *Information Privacy and the Information Economy*, 117 NW. U. L. REV. 357, 362 (2022).

[107] Viljoen, *supra* note 25, at 578; *see also* Matsumi & Solove, *supra* note 103 (manuscript at 47).

Model and that are much more aligned with the Societal Structure Model.[108] The new European Union Artificial Intelligence Act ("EU AI Act") is a milestone in this direction.[109] Instead of relying heavily on individual rights, the law sets forth a risk-based approach that provides protection without placing the onus on individuals.[110] Certain deployments of AI are heavily restricted or outright prohibited.[111] We are encouraged by this style of regulation, which will hopefully harbinger a new direction for AI.

New AI regulation is an important step forward, but existing privacy law must also be reworked to focus more on the Societal Structure Model. AI overlaps with privacy significantly, but there are still many AI issues that don't involve privacy, and vice versa. There are a myriad of instances of data collection, use, and disclosure beyond AI where individual control is inadequate as a regulatory response. We thus caution against AI exceptionalism; the Societal Structure Model should be embraced broadly for privacy regulation, whether AI is involved or not.

Both of us have long argued for many steps privacy law can take to embrace the Societal Structure Model. For example, we have contended that the law should draw from the law of fiduciaries to impose duties on large organizations that collect and use our data.[112] These organizations should be understood as

[108] *See* Digital Consumer Protection Commission Act of 2023, S. 2597, 118th Cong. §§ 2411-14 (2023) (proposing duties of loyalty, care, confidentiality, and mitigation); Press Release, Sen. Elizabeth Warren, Warren, Graham Unveil Bipartisan Bill To Rein in Big Tech, (July 27, 2023), https://www.warren.senate.gov/newsroom/press-releases/warren-graham-unveil-bipartisan-bill-to-rein-in-big-tech [https://perma.cc/XDY9-MXYW] (discussing Digital Consumer Protection Commission Act of 2023 that established commission to regulate online platforms); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022) ("A Bill To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement."); Data Care Act of 2021, S. 919, 117th Cong. (2021) ("A Bill To establish duties for online service providers with respect to end user data that such providers collect and use.").

[109] European Parliament Press Release, Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI (Sept. 12, 2023, 12:04 AM), https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai [https://perma.cc/A3YL-CTR9] (discussing AI Act's main regulatory features and its progress toward formal adoption into law, including European Parliament and Council provisional agreement.)]

[110] For background about the new EU AI Act, see *Artificial Intelligence—Questions and Answers*, EUR. COMM'N (Dec. 12, 2023), https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683. For a tremendously insightful discussion of risk-based AI regulation, see Margot E. Kaminski, *Regulating the Risks of AI*, 103 B.U. L. REV. 1347 (2023).

[111] European Parliament Press Release, *supra* note 109.

[112] *See* SOLOVE, THE DIGITAL PERSON, *supra* note 1, at 102-04 (arguing fiduciary relationship between companies and individuals should be based on the factors courts traditionally consider when determining fiduciary relations); Richards & Hartzog, *Duty of Loyalty*, *supra* note 24, at 964 (arguing some duty of loyalty should be imposed upon companies collecting and processing human information); Richards & Hartzog, *Taking Trust*

trusted parties or *information fiduciaries*. One of the most important aspects of a fiduciary and trust approach to information privacy is the idea that the powerful companies that invoke people's trust should be prohibited from acting in ways that conflict with the trusting parties' best interests. This is not a novel legal approach. It's how the law deals with lopsided relationships where one party has all the power and information and the other is made vulnerable as a result.

The ultimate story is power. Digital technology is changing the dynamic of power in ways that threaten individuals. But Kafka shows us that empowering individuals is agonizingly complicated. Kafka's darkly comedic view of human nature is brutally candid and peers unblinkingly into the shadows of the human psyche.

In the end, if we reap one key insight from Kafka's work for how to regulate privacy in the age of AI, it is this: *the law won't succeed in giving individuals control; instead, the law must try to control the larger forces that exploit people and to protect individuals, communities, and society-at-large from harm*.

CONCLUSION

Writing more than a century ago, Kafka couldn't have been a more fitting prophet for our times today. If we accept Kafka's worldview, however, how do we avoid falling into despair? Is there a way out?

In *A Little Fable*, Kafka writes of a mouse who keeps running from one room to the next.[113] The mouse says that "the world is growing smaller every day. At the beginning it was so big that I was afraid."[114] The mouse keeps running and now notes that "these long walls have narrowed so quickly that I am in the last chamber already, and there in the corner stands the trap that I must run into."[115] The last line of the parable follows quite suddenly and abruptly: "'You only need to change your direction,' said the cat, and ate it up."[116]

Today, technology titans are racing to develop new technologies that are gathering and analyzing massive quantities of data about us. Despite the enactment of privacy laws around the world, we're still heading toward a trap.

The Individual Control Model is a dead end. Although many policymakers and commentators know this, they keep returning to it. It's the classic Kafka plot: people know their quest is doomed and yet persist with it anyway.

Seriously, *supra* note 24, at 457 (arguing to implement fiduciary duties in context of privacy law); *see also* Balkin, *Fiduciary Model of Privacy*, *supra* note 24, at 1186 (arguing online service providers who collect and distribute personal information should be classified as information fiduciaries); Balkin, *Information Fiduciaries*, *supra* note 24, at 11 (arguing digital companies that collect and use personal data should be treated as fiduciaries to their end users).

[113] FRANZ KAFKA, A LITTLE FABLE (Willa Muir & Edwin Muir trans.) (1931), *reprinted in* THE COMPLETE STORIES 492, 492 (Nahum N. Glatzer ed., 1971).

[114] *Id.*

[115] *Id.*

[116] *Id.*

In Kafka's world, the mouse doesn't change direction, and it meets an untimely demise. Let's hope in our world, policymakers won't keep making the same mistake.