VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SUMMER 2022 UNIVERSITY OF VIRGINIA VOL. 26, NO. 2

"NOBODY IS WATCHING ME": TOWARDS HUMAN-CENTRIC PRIVACY AND HUMANLESS INFORMATION PROTECTION

Yafit Lev-Aretz[*]

[*] Assistant Professor of Law, The Zicklin School of Business, Baruch College, City University of New York, and Director of Tech Policy, The Robert Zicklin Center for Corporate Integrity, Baruch College, City University of New York. For helpful comments and insights on earlier drafts, the author would like to thank Kiel Brennan Marquez, Ignacio Cofone Amit Elazari, Ira Rubinstein, Tomer Kenneth, Amanda Levendowski, Helen Nissenbaum, Shannon K. O'Byrne, Paul Ohm, Gideon Parchomovsky, Julia Powles, Ira Rubinstein, Madelyn R. Sanfilippo, Katherine Strandburg, Daniel Susser, Ari E. Waldman and the participants of the *Information Law Institute Privacy Research Group* at NYU Law School, the Academy of Legal Study of Business Annual Conference, the Princeton Center for Information Technology Policy TecSoc group, and the *Privacy Law Scholars' Conference*, Berkeley, CA, June 2019.

Abstract

Despite gaining renewed interest, privacy keeps struggling with puzzling dynamics like the privacy paradox, continuously fails as a policy goal, and lacks an operationalizable definition. Scholarly attempts to explain the failure of privacy policymaking have highlighted the conceptual and practical disarray around privacy law. This Article identifies an additional overlooked cause: Privacy regulation has been designed around the increasingly faulty premise that non-consensual observation by other humans is the paradigmatic privacy harm. Privacy law has evolved with a human-centric approach, assuming the presence of a human observer and a human observed. Information technologies, however, have made information flows humanless, with an algorithm instead of a human observer and a data point representing the human subject. To cover humanless information flows and to address surveillance that bypasses human limitations, the scope of privacy has been gradually expanding. The traditional human-centric model, however, has failed to capture the broader implications of humanless surveillance and turned privacy into an inflated and ill-defined concept.

Following a detailed account of the human-centric development of privacy law, this Article shows how overbroad privacy is failing conceptually and strategically. To remedy this failure, this Article argues that privacy law must be kept human centric, while information protection laws move away from the human centric paradigm. Differentiating between human and humanless informational harms is crucial for effective policymaking as it renders the notice and consent model insufficient, points us toward the legitimacy of information flows as the key policy question, and invites different kinds of strategies for political mobilization.

TABLE OF CONTENTS

II. PRIVACY AND THE HUMAN ELEMENT 3

III. THE LEGAL RIGHT TO PRIVACY AND THE HUMAN ELEMENT 11
A. EARLY VIEWS ON THE RIGHT TO PRIVACY 11
B. HUMAN CENTRIC PRIVACY TORTS 13
C. THE FOURTH AMENDMENT 14
D. REGULATION OF DE-IDENTIFIED OR ENCRYPTED DATA 17

IV. THE FAILURE OF OVERBROAD PRIVACY 19
A. PRIVACY'S CONCEPTUAL FAILURE 19
B. PRIVACY'S STRATEGIC FAILURE 22
i. Users' Privacy and the Human Element 22
ii. Lawmakers' Privacy Views 25
iii. Silicon Valley and Privacy Whitewashing 27

V. DECOUPLING PRIVACY FROM HUMANLESS INFORMATIONAL HARMS 29
A. NO PRIVACY CIRCUIT – NO PRIVACY VIOLATION 29
B. CONSENT AND HUMAN PRIVACY MYOPIA 31
C. SAME PROBLEMS – DIFFERENT, MORE EFFECTIVE LEGAL TOOLS 32

II. VI. CONCLUSION 35

I. INTRODUCTION

We live in a state of privacy disorientation. Privacy scandals are announced on a weekly basis, yet personal information continues to fuel the data economy. When asked about privacy preferences, consumers claim to assign great value to privacy, but individual behavior has not matched those self-reported privacy values. Exemplifying what scholars have referred to as the privacy paradox, consumers rush to share information, click "I Agree," sign up to additional services, and purchase more products that collect and monetize personal information.[1]

Even in the face of the General Data Protection Regulation (GDPR)[2] in Europe, a growing number of federal privacy bills,[3] and some relatively successful states privacy laws[4] the challenge that Professor Priscilla Regan identified over 25 years ago still stands: Privacy has been failing as a policy goal.[5] This continuous failure may indicate, as some have argued, that privacy ranks low in our societal and legal priorities.[6] This Article

---

[1] The striking difference between theoretical positions and actual behaviors around privacy has been referred to as the "privacy paradox." *See* Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors,* 41 J. CONSUMER AFF. 100, 101, 108-13 (2007); Patricia A. Norberg & Daniel R. Horne, *Privacy Attitudes and Privacy-Related Behavior*, 24 (10) PSYCHOL. & MARKETING 829 (2007); C. B. Paine & A.N. Joinson, *Privacy, Trust and Self-Disclosure*, in PSYCHOLOGICAL ASPECTS OF CYBERSPACE: THEORY, RESEARCH, APPLICATIONS (A. Barak ed., 2008); Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox-Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior--A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038 (2017); Monika Taddicken, *The "Privacy Paradox" in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure*, 19 J. COMPUTER-MEDIATED COMMUN 248, 265-68 (2014), and Idris Adjerid et al., *The paradox of wanting privacy but behaving as if it didn't matter*, LSE BUS. REV. (2018), https://blogs.lse.ac.uk/businessreview/2018/04/19/the-paradox-of-wanting-privacy-but-behaving-as-if-it-didnt-matter/.

[2] 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, 2018 O.J. L 119 [hereinafter, GDPR].

[3] Federal Privacy Bills – 116th and 117th Congresses, in both chambers: Public Health Emergency Privacy Act, S. 3749, 116th Cong. (2020);
Promoting Digital Privacy Technologies Act, S. 224, 117th Cong. (2021);
Protecting Investors' Personally Identifiable Information Act, H.R. 2039, 117th Cong. (2021);
Protecting Consumer Information Act of 2021, H.R. 474, 117th Cong. (2021);
Information Transparency & Personal Data Control Act, H.R. 1816, 117th Cong. (2021);
Data Care Act of 2021, S.1444 - Mind Your Own Business Act of 2021, S. 919, 117th Cong. (2021);
Children and Teens' Online Privacy Protection Act, S. 1628, 117th Cong. (2021);
Social Media Privacy Protection and Consumer Rights Act of 2021, S. 1667, 117th Cong. (2021);
Data Protection Act of 2021, S. 2134, 117th Cong. (2021).

[4] California enacted SB-1121 California Consumer Privacy Act of 2018 (CCPA). In 2021, Colorado enacted the Protect Personal Data Privacy (2021) and Virginia passed SB 1392 Consumer Data Protection Act; personal data rights of consumer, etc. (2021). Other states, including New York, Massachusetts, North Carolina, and Pennsylvania, have proposed digital privacy legislation, see Sarah Rippy, *US State Privacy Legislation Tracker*, IAPP https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ .

[5] Priscilla M. Regan, Legislating Privacy 1-24 (1995).

[6] *See, e.g.*, Caleb Fuller, *How Consumers Value Digital Privacy: New Survey Evidence*, GEO. MASON U.: PROGRAM ON ECON. & PRIVACY (Feb. 20, 2018), https://pep.gmu.edu/wp-content/uploads/sites/28/2018/02/Fuller_How-Consumers-Value-Digital-Privacy.pdf. Robert W. Hahn & Anne Layne-Farrar, *Is More Government Regulation Needed*

advances an alternative explanation: Our privacy laws, institutions, and norms have evolved with a clear notion of *human presence*, a human observer and a human observed. Technology, however, has created a new form of observation – one that is *humanless*. And while tech companies are said to be constantly watching us, it is in fact quite rare that *a human is watching us*. More often than not, *nobody* is watching, because the information is collected automatically and processed through algorithmic systems. More often than not, nobody is watching *us* because our identity in the collection process is often obscured and represented through numerical expressions or data points.

Privacy has been failing as a policy goal because privacy regulation has been designed around what over time turned to be a faulty premise, that non-consensual observation by other humans is the paradigmatic privacy harm. But technology has taken us away from the human watching model. Privacy's problems have gone from peeping toms to cases of algorithmic spying. Yet, the way we talk, think, and practice privacy still follows the traditional human-centric paradigm.

The turn to privacy in the face of humanless surveillance makes intuitive sense: The harms of humanless surveillance do resemble many of those presented by human surveillance, as both involve information-driven power of the observer, as well as helplessness and vulnerability of the observed. Furthermore, because humanless tracking is intended to produce personal information-driven insights, and because just like human surveillance, humanless tracking revolves around personal information-driven power, privacy seems to offer the best toolbox to address the challenges of humanless surveillance. And so, in the past two and a half decades, the privacy discourse has entered new, humanless, domains, which have not been traditionally concerned with privacy. The expansion of the human-centric privacy model into humanless information flows has resulted in a scattered, incoherent, and highly disoriented privacy discourse. Over time, the privacy concept has grown to encompass any conceivable information-related issue including profiling, discrimination, manipulation, algorithmic bias and error, unjust enrichment, content moderation, and excessive market power.[7]

Unfortunately, turning to privacy to address neighboring informational harms has been proven unhelpful and even harmful. In many of those informational harms the privacy interest is attenuated, especially when compared with other values. Resorting to privacy rhetoric not only has turned privacy into an all-encompassing (thus mostly toothless) right but has also distracted from the development of relevant legal doctrines to address new informational harms. Take for example the Cambridge-Analytica scandal, which was dominantly framed as a privacy violation.[8] Personal information about millions of users was

---

to Promote E-Commerce?, 35 CONN. L. REV. 195 (2002) (noting in the context of online shopping that "[t]here is no evidence that any e-commerce has been deterred. Absent evidence of a significant market failure, the case for further government intervention is weak at best"). *See also* Solveig Singleton*, Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. 97, 147 (2000).

[7] Natasha Singer, *Just Don't Call It Privacy,* N.Y. TIMES, Sep. 22, 2018, https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html.

[8] Maya Kosoff, *"Cambridge Analytica is Just the Tip of the Iceberg": Why the Privacy Crisis is Bigger Than Facebook,* VANITY FAIR, Apr. 16, 2018, https://www.vanityfair.com/news/2018/04/why-the-privacy-crisis-is-bigger-than-facebook; Nick Statt, *Mark Zuckerberg Apologizes for Facebook's Data Privacy Scandal in Full-Page Newspaper Ads*, THE

accessed without authorization. However, personal information is commonly accessed and used, even when authorization formally exists, without real knowledge or meaningful consent. Were we truly raging over Facebook's failure to detect the uninvited guest who crashed our personal information feast when we've never paid attention to the guest list?[9] As many have identified later, the privacy violation in the Cambridge Analytica scandal was secondary and pale compared to other harms like voter manipulation and election meddling.[10]

The divergence from the human-centric model has been instrumental in the failure of privacy as a policy goal. Users and regulators alike have struggled to reconcile their intuitions around human-centric privacy with their choices around humanless surveillance. To effectively address both human and humanless informational harms, I argue that privacy must remain human-centric and narrow. The value of identifying human surveillance as involving a privacy interest and humanless surveillance as a data protection issue goes beyond rhetorical clarity. It involves at least three beneficial changes the current data protection regulatory discourse: Rendering the notice and consent model insufficient; highlighting the legitimacy of information flows as the key question and inviting different kinds of strategies for political mobilization.

The rest of the Article unfolds as follows: part II explains the theory of privacy as a human centric concept. Part III tells the evolutionary story of the legal right to privacy and highlights the human presence in privacy laws and institutions. Part IV moves to illustrate the downsides of using privacy as an all-inclusive term to describe all informational issues, and Part V advocates for using privacy in a narrower sense to better protect against both human-centric privacy violations *and* humanless information-driven harms. A conclusion follows.

II. PRIVACY AND THE HUMAN ELEMENT

In an oft-cited 2001 work, Daniel Solove explained why the big brother metaphor, referencing George Orwell's book, 1984, is ill suited to describe the data collection problem.[11] During that time, as information technologies gradually became more common,

---

VERGE, Mar. 25, 2018, https://www.theverge.com/2018/3/25/17161398/facebook-mark-zuckerberg-apology-cambridge-analytica-full-page-newspapers-ads; Tara Fowler, *Facebook Announces Overhaul of Security and Privacy Settings in Wake of Cambridge Analytica Scandal*, ABC NEWS, Mar. 28, 2018, https://abcnews.go.com/Technology/facebook-announces-overhaul-security-privacy-settings-wake-cambridge/story?id=54055454, and Nellie Bowles, *After Cambridge Analytica, Privacy Experts Get to Say 'I Told You So*,' N.Y. TIMES, Apr. 12, 2018, https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html.

[9] Yafit Lev-Aretz, *Facebook and the Perils of Personalized Choice Architecture*, TECHCRUNCH, Apr. 2018, https://techcrunch.com/2018/04/24/facebook-and-the-perils-of-a-personalized-choice-architecture/.

[10] Tal Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES IN LAW 157, 169 (2019); Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 467 (2019); Daniel Susser, Beate Roessler, Helen Nissenbaum, *Online Manipulation: Hidden Influences in A Digital World,* 4 GEO. L. TECH. REV. 1 (2019); Patrick Day, *Cambridge Analytica and Voter Privacy*, 4 GEO. L. TECH. REV. 583 (2020), and Margot E. Kaminski, *Binary Governance: Lessons from the Gdpr's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1544 (2019)

[11] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1393 (2001).

Solove realized that something about the conceptualization of privacy was not working. "[T]he Big Brother metaphor as well as much of the law that protects privacy", observed Solove, "emerges from an older paradigm for conceptualizing privacy problems" as "uncovering one's hidden world, by surveillance, and by the disclosure of concealed information."[12] Privacy violations, under this paradigm, lead to harms like inhibition, self-censorship, embarrassment, and reputational damage.[13] Solove continued to claim that because privacy law has developed with this big brother paradigm in mind, privacy law has failed to address what Solove called "the database problem."[14] As a better alternative, Solove proposed Franz Kafka's depiction of bureaucracy in *The Trial*, which pictures a world of "bureaucratic indifference, arbitrary errors, and dehumanization… where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of their information."[15]

Back in 2001, Solove forecasted many of the informational problems that challenge society today, over two decades later. Solove perfectly captured the broader implications of the database problem and while he did not discount the harms under the 1984 metaphor, he highlighted an additional, and in the context of databases, more pressing set of concerns:

> "The most insidious aspect of the surveillance of Big Brother is missing in the context of databases: *human judgment about the activities being observed (or the fear of that judgment).* Surveillance leads to conformity, inhibition, and self-censorship in situations where it is likely to involve human judgment. Being observed by an insect on the wall is not invasive for privacy; rather, privacy is threatened by being subject to human observation, which involves judgments that can affect one's life and reputation… Much personal information is amassed and processed by computers; we are being watched not by other humans, but by machines, which gather information, compute profiles, and generate lists for mailing, emailing, or calling. This impersonality makes the surveillance less invasive."[16]

While Solove did not go on to develop a full theory of privacy around the gradual elimination of the human element, he certainly identified the shift to humanless surveillance as a fundamental change that goes to the heart of the privacy interest. This Article continues where Solove left off to argue that our privacy norms, and consequentially our laws, have traditionally revolved around human observation and subsequent judgment. With the advantage of twenty additional years of information technology development, this Article demonstrates how the dominance of the human-centric model have been instrumental in

[12] *Id.*

[13] *Id.* at 1417-18.

[14] *Id.* at 1418-19.

[15] *Id.* at 1398.

[16] Solove, *supra* note 11 at 1417-18.

undermining privacy as a policy goal, and in distracting from addressing other informational harm.

In a Washington Post editorial published four years after Solove's work, Judge Richard Posner voiced a similar and somewhat bolder view:

> The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.[17]

In his editorial, Posner advocated for greater government access to information contained in e-mails, phone conversations, and banking records of U.S. citizens, citing the need to prevent terrorist attacks. Specifically, he argued that "(t)he government is entitled to those data, but just for the limited purpose of protecting national security."[18] Posner's intuition, while not clearly stated, is clear. Scrutinizing government access to personal data is key, but mostly because of the crucial need to place checks on government powers, and not because such access represents a severe privacy violation.

To better conceptualize the human-centric model versus the humanless approach, this Article suggests a useful metaphor: a privacy circuit. In many ways, traditional views of privacy are analogous to an electric circuit – just like electric circuits require a positive terminal and a negative terminal to be closed, a privacy violation has traditionally required a human observer and a human observed to fully materialize. Information technology and the automation rush, however, have growingly excluded humans from the information circuit. The human detachment is not an incidental byproduct – it is the goal. The lesser the human role in the circuit, the more the process is regarded effective and cutting edge.

Human involvement is successfully minimized in the observing end, namely – in the information collection and use process. Traditionally, humans collected information about other humans, memorized it or otherwise remembered it with the help of labor-intensive recording means. Humans also had to make sense of the collected information and analyze it to come up with useful insights. Those insights would then be logged in human memory or other forms of analog documentation and be pulled out to inform human decision making as needed. With information technologies, information storage and retrieval are no longer dependent on limited human cognitive abilities. Information collection technologies constantly improve and are commonly capable of offering fully automated collection of information. Data analysis has also departed from human participation: models run automatically on massive troves of data. Machine learning technologies can further minimize human involvement, as they improve by self-learning

---

[17] Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST Dec. 21, 2005, https://www.washingtonpost.com/archive/opinions/2005/12/21/our-domestic-intelligence-crisis/a2b4234d-ba78-4ba1-a350-90e7fbb4e5bb/.

[18] *Id.*

that not only lacks a human touch by design, but at times is also so complex and opaque even to a trained human eye.[19] And as decision-making also moves towards automation, the entire process can be completed without human involvement.

The observed end, namely – the data subject about whom information is collected and analyzed – also becomes growingly humanless. As Solove rightly observed: "Since marketers generally are interested in aggregate data, they do not care about snooping into particular people's private lives"[20] and as a result "we are reconstituted in databases as a digital persona composed of data."[21] It is not the self that is valued in a database; it is the data that the self generates. In other words, the fuel of today's information economy is not the data subject – it is the data point. It is much like the correlation between image quality and the number of pixels: Each pixel on its own is meaningless, but when placed correctly with other pixels it can tell a detailed story. Similarly, the value of a data subject is only evaluated in relation to its part in a big picture. As a result, individuals often feel, and rightly so, that they are safely lost in the crowd. Unless specifically sought after, information about an individual data subject is obfuscated in a database, turning the individual self into a faceless building block.[22]

The shift from human observation and judgment of another human to an algorithmic observation of data points has changed the way people think about sharing information. To some extent, individuals lack understanding of the far-reaching implications of data collection and use.[23] To some extent, they also feel helpless in the face of ubiquitous surveillance.[24] But to some extent, which has been virtually overlooked by legal commentary, individuals do not feel that they are being watched. Many of them feel like they are not of special interest to the data collector. *Nobody* is watching *them.* Sometimes, when people get creepy reminders that they are being watched, such as when cookies follow them as they move from one website to another, they voice their concern and outrage. But when realizing it is all automated and that no human is tracking their online behavior, many feel safe again and the tracking is normalized.

Cases of human intervention in otherwise commonly automated processes involve a privacy violation that is reflected in users' reactions. Take for example smart speakers and home virtual assistants such as Amazon's Alexa and Google home. While most people are unlikely to bring a human assistant that records all interactions into the private parts of

---

[19] See, e.g., Katherine J. Strandburg, Rulemaking and Inscrutable Automated Decision Tools, 119 COLUM. L. REV. 1851 (2019); Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 GEO. L.J. 1147, 1159 (2017); Andrew D. Selbst & Solon Barocas, The Intuitive Appeal of Explainable Machines, 87 FORDHAM L. REV. 1085 (2018), and Jeanne C. Fromer, Machines as the New Oompa-Loompas: Trade Secrecy, the Cloud, Machine Learning, and Automation, 94 N.Y.U. L. REV. 706 (2019).

[20] Solove, *supra* note 11 at 1418.

[21] *Id.* at 1425.

[22] This, together with privacy law individualism had resulted in the omission of data relations from current data governance regimes, Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 592-603, 609-17 (2021).

[23] Yafit Lev-Aretz & Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, 22 YALE J.L. & TECH. 256, 284-87 (2020).

[24] A. Michael Froomkin, Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements, 2015 U. ILL. L. REV. 1713, 1736 (2015).

their home, nonhuman virtual assistants have gained significant traction so far.[25] When stories about human intervention break, users' reactions as well the way the media frames those interventions, highlight that human intrusions represent a different kind of privacy violation. A Bloomberg report about Amazon's global team reviewing Alexa audio clips have dominated the news for nearly a week, with various stories and opinion pieces explaining the risk and offering mitigations.[26] But if it is the mere act of listening and recording that is troubling, why does it matter that this act was occasionally assigned to humans? It does, because humans form judgment when exposed to information about other humans, and even though the reviewed voice recordings were anonymized, this type of information flow was communicated and analyzed as a different, more disturbing, privacy violation. As the L.A. Times aptly put it when reporting about the story: "Alexa may be listening, but will she tell on you?"[27] Before a human enters the loop, we tend to care significantly less about being observed.

While many information flows today exclude humans from the loop, many of them still require human involvement. The Alexa voice review story highlights that the human role in training software algorithms has not died out. Smart algorithms improve by learning from experience, but humans are still responsible for a fair amount of teaching. In addition, humans can enter the loop illegitimately. On the observing end, even if data collection is completely automated, rogue employees can access information about users without authorization.[28] On the observed end, hacking and information leaks can identify individuals who are otherwise obscure in the database as the aftermath of the Yahoo,[29]

---

[25] Sarah Perez, *Smart speaker sales reached new record of 146.9M in 2019, up 70% from 2018*, TECHCRUNCH, Feb. 17, 2020, https://techcrunch.com/2020/02/17/smart-speaker-sales-reached-new-record-of-146-9m-in-2019-up-70-from-2018/.

[26] Matt Day, Giles Turner & Natalia Drozdiak, *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG, Apr. 10, 2019, https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio. *See also* Kyle Wiggers, *How Amazon, Apple, Google, Microsoft, and Samsung Treat Your Voice Data*, VENTURE BEAT, Apr. 15, 2019, https://venturebeat.com/2019/04/15/how-amazon-apple-google-microsoft-and-samsung-treat-your-voice-data/; T. J. McCue, *Alexa Is Listening All The Time: Here's How To Stop It*, FORTUNE, Apr. 19, 2019, https://www.forbes.com/sites/tjmccue/2019/04/19/alexa-is-listening-all-the-time-heres-how-to-stop-it/#7f9c0f9f5e2d, and Alyssa Newcomb, *The 'Less Sexy Side' of A.I.: Why Amazon Employees Are Listening to What You Tell Alexa,* FORTUNE, Apr. 13, 2019, http://fortune.com/2019/04/13/alexa-ai-amazon-privacy-artificial-intelligence-smart-home/.

[27] Agatha French, *Alexa May Be Listening, But Will She Tell on You?,* L.A. TIMES, Jan. 5, 2017, https://www.latimes.com/business/technology/la-fi-tn-amazon-echo-privacy-qa-20170105-story.html.

[28] For instance, Facebook and Uber detected instances of employees who used their privileged access to stalk users and especially women. *See* Ben Popken, *Facebook Fires Engineer Who Allegedly Used Access to Stalk Women*, NBC NEWS, May 1, 2018, https://www.nbcnews.com/tech/social-media/facebook-investigating-claim-engineer-used-access-stalk-women-n870526; Avery Hartmans, *Uber Employees Used the Platform to Stalk Celebrities and Their Exes, A Former Employee Claims*, BUSINESS INSIDER, Dec. 12, 2016, https://www.businessinsider.com/uber-employees-stalked-celebrities-ex-employee-claims-2016-12.

[29] Selena Larson, *Every Single Yahoo Account Was Hacked - 3 Billion in All*, CNN, Oct. 4, 2017, https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html. Current settlement efforts reach $117.5 million. Kara Yurieff, *Yahoo Tries Again to Settle Lawsuit Over Massive Data Breach. This Time it Offers $118 Million,* CNN, Apr. 9, 2019, https://www.cnn.com/2019/04/09/tech/yahoo-data-breach-settlement/index.html.

Equifax,[30] and Marriott[31] data breaches showed. Beyond identity theft, fraud, and other safety risks, sometimes the mere identification of an individual in certain databases can result in severe privacy harm.[32] It is still the presence of human observation and subsequent judgment that brings the informational harm within the purview of a privacy harm, but as these examples show, humans may enter the loop unexpectedly or illegitimately at any time. Indeed, various data protection means can minimize such unexpected or illegitimate human intrusion as well as the resulting privacy harm. Limiting collection, retention time, and sharing of personal data with third parties can all cut down both the instances of privacy invasions and the harm they impose on the exposed individuals. Under the theory advanced here, however, it is not until humans enter the privacy circuit at both ends – the observer and the observed – that a privacy violation has materialized.

Importantly, not every instance of a closed privacy circuit equals a privacy violation. After all, humans observe humans all the time and in most instances the observation is socially acceptable and does not result in a privacy violation. Social norms determine which observations constitute privacy violations and which are legitimate. The contextual integrity framework, which assesses the appropriateness of information flows based on their agreement with contextual norms,[33] offers useful tools to pinpointing the social norm and recognizing violation. In other words, the closed privacy circuit with humans on both ends is a prerequisite to labeling an information flow a privacy violation. Relevant information norms and the context should be further reviewed to establish privacy violation.[34]

Furthermore, line drawing around what should be considered a human observer and what should be considered an identified observed human is a quite challenging task. While humans may feel invaded when watched by other humans, they also feel invaded when watched by non-humans who sound, look, or otherwise feel like humans. Indeed, with the

---

[30] Alfred Ng & Steven Musil*, Equifax Data Breach May Affect Nearly Half the US Population*, CNET Sep. 7, 2017, https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/. For the Government Accountability Office (GAO) report that was published a year after the reported breach and which details how the credit monitoring company was hacked see U.S. GOV'T ACCOUNTABILITY OFF. GAO-18-559, ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH, (2018),https://www.gao.gov/assets/700/694158.pdf.

[31] Taylor Telford & Craig Timberg, *Marriott Discloses Massive Data Breach Affecting Up to 500 Million Guests*, WASH. POST, Nov. 30, 2018, https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/?noredirect=on&utm_term=.5b9884f66924.

[32] For example, individuals whose information was exposed in the course of the Ashley Madison (infidelity dating site) security breach could suffer severe consequences, including public humiliation, job loss, divorce and financial ruin. Jessica Elgot, Alex Hern & Matthew Weaver, *Ashley Madison Adultery Site Hack: Will I Be Found Out?,* THE GUARDIAN, July 21, 2015, https://www.theguardian.com/world/2015/jul/21/ashley-madison-adultery-site-hack-will-i-be-found-out-what-you-need-to-know ("Millions of users of the infidelity website may have good reason to be worried as cybercrime experts warn that 'Impact Team' may be focused on blackmail"). *See also Ashley Madison Cheaters List Now Searchable by Name and Email,* WGNO ABC, Aug. 20, 2015 https://wgno.com/2015/08/20/ashley-madison-cheaters-list-now-searchable-online-2/.

[33] Helen Nissenbaum, Privacy in Context 129-158, 186-230 (2010).

[34] An information flow may be deemed illegitimate even when the information flowing is non-personal information, non-identified information, and even information about corporations and non-living. Thus, under the argument advanced in this work, and to a large extent under the common understanding of the contextual integrity theory, the contextual integrity theory stains illegitimate information flows even when they do not violate privacy if they violate other contextual norms and value.

growing use of virtual assistants, robots, and other interactive smart devices, human-like machines become mainstream. Communications and psychology scholarship suggest that technologies exhibiting anthropomorphic qualities, from language and voice to physical symbols like eyes and hands, elicit responses that are associated with being in the presence of other humans.[35] Associated behaviors such as politeness, self-consciousness, self-promotion, and self-censorship, all indicate that even when people know they interact with a machine, at a visceral level they get the feeling of being observed and evaluated.[36] At times, the human-like behavior of the machine is so persuasive that individuals may not realize that they interact with a machine. Should the fact that an individual has been observed by someone who displayed human qualities but was in fact a non-human change the way we evaluate the privacy circuit? Does it matter if the observed knew that he or she is watched by a non-human, but the persuasive human-like behavior of the robot made the observation feel human? One approach evaluates the information practice based on user experience without applying any objective standard to the user experience: if users feel that they interact with a human, regardless of whether they knew or should have known that they interact with a machine, a privacy interest is implicated.[37] While I acknowledge the importance of those questions, they require a deep normative analysis that exceeds the scope of this work.

Similarly, when referring to observed humans, I admittedly refer to clear extreme cases in which the observed are clearly identified in a manner that implicates a privacy interest. Nevertheless, there is a spectrum. When would a data subject move from being a data point to being identified as him or herself? Is the mere revealing of one's name meaningful when the human observer on the other end does not know the observed? Is an email address sufficiently telling to materially expose individuals? Are visuals somehow different? When observed by a human, is a person's face without additional identifying information enough to turn that person into an observed human? And what about a picture/video of an individual's private parts without a face or other identifying information? These questions involve deep philosophical and social approaches as to what makes us who we are and what we consider to be parts of our unique self and identity. Some questions were occasionally dealt with in the context of the appropriation tort,[38] and in attempts to distinguish personal from non-personal information.[39] But no clear lines have

---

[35] M. Ryan Calo, People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship, 114 PENN ST. L. REV. 809, 835-42 (2010).

[36] *Id.* at 838-42.

[37] This is the approach advocated for by Calo. *Id.* at 842-50.

[38] *See infra* part III b, and Prosser's line-drawing explanations of appropriation: "It is the plaintiff's name as a symbol of his identity that is involved here, and not his name as a mere name… It is not enough that a name which is the same as his is used in a novel, a comic strip, or the title of a corporation, unless the context or the circumstances, or the addition of some other element, indicate that the name is that of the plaintiff." And he further notes that "there is no liability for the publication of a picture of his hand, leg and foot, his dwelling house, his automobile, or his dog, with nothing to indicate whose they are." William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 403-05 (1960).

[39] In a 1998 work, Jerry Kang argued that information is "identifiable to an individual" when it bears "(1) an authorship relation to the individual, (2) a descriptive relation to the individual, or (3) an instrumental mapping relation to the individual." Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1206-07

been drawn to establish a turning point in which a human is meaningfully identified. An in-depth study of the human self-spectrum exceeds the scope of this work. Thus, this Article acknowledges this missing part of the theory, which is important but not indispensable to establish the hypothesis.

The argument presented here is largely dependent on privacy views and other norms at a given point in time. In the past, for instance, royals would rarely attach intrusive quality to the presence of their servants notwithstanding the fact that those servants were observing them and forming a judgment. This relative comfort is a result of a specific social structure, under which servants were considered sub-human and their observation did not bear any social consequences. Exposing one's body next to a servant would oftentimes equal striping next to a pet. Just like a pet, a servant might be watching and forming a judgment, but that observation and judgment carried no social value or consequences in the royals' world.

The understanding that our privacy views are strongly tied to our social norms is not new and makes a lot of sense.[40] But in the context of privacy and the human element, more than a minor adjustment to technological changes will be needed to move us away from attaching social consequences to human observation and judgment. A shift would be momentous and may materialize by either eliminating the emotional and social power of human observation or by extending that same power to machine observation. In other words, we will either become sufficiently accustomed to human observation and judgment that we will no longer assign any emotional and social consequences to it, or we will start attaching an emotional and social price to non-human observation.[41] Judging by the current state of information markets and automation incentives, the former is highly unlikely. We will probably see less and less human observation in data collection and use as processes, including decision-making and execution become (truly) fully automated. The latter, however, is possible. As technology moves toward pushing humans out of the loop, it also moves towards making technological agents more human-like. If artificial intelligence gains the ability to form meaningful judgment – a possibility that currently seems highly far-fetched – then individuals might start attaching social value to observation by machines. In such case, our definition of privacy harm would have to change accordingly. Even if machines cannot truly form observation-driven judgments but have a sufficiently convincing appearance of making such judgments, our privacy norms would change to reflect the level of discomfort individuals encounter when information about them is observed by a machine.

(1998). While it still suffers from blind spots and vagueness, this approach offers a promising starting point to answering the question of what should qualify as human identification.

[40] This is the whole premise of the contextual integrity theory, which highlights the importance of entrenched informational norms. NISSENBAUM, *supra* note 33.

[41] *See, e.g.*, Ian Kerr, *Schrödinger's Robot: Privacy in Uncertain States*, 20 THEORETICAL INQUIRIES L. 123, 127-28 (2019) (arguing that privacy is relational, "namely: a person loses privacy just in case some "other" gains some form of epistemic access to her." While the "other" was historically conceived as the observing person, Kerr argues that "robots and AIs are replacing the human "other" and that the delegation of informational transactions to robots and AIs therefore puts the traditional privacy relationship in an uncertain state.")

The next part follows the above outlined development of the human-centric privacy theory by reviewing the legal evolution of the right to privacy. It demonstrates how our privacy norms and privacy laws have developed through a human-centric approach.

III. THE LEGAL RIGHT TO PRIVACY AND THE HUMAN ELEMENT

a. Early Views on the Right to Privacy

In 1890, a foundational article by Samuel Warren and Louis Brandeis titled "The Right to Privacy," first conceptualized the right to privacy as "the right to be left alone."[42] Warren and Brandeis recognized that existing legal causes of action at the time did not effectively protect privacy but that courts could use existing legal concepts from the common law to develop legal protection for "some retreat from the world."[43] The historical context confirms that Warren and Brandeis had viewed the privacy interest as operating only within the context of human interaction. The personal motivation behind this article was Warren's own experience with an intrusive press, which found his private life of great interest because he married a senator's daughter.[44] The technological motivation behind the article was the mass marketing of Kodak's portable camera and the subsequent rise of gossip journalism.[45] Warren and Brandeis cautioned that

> "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' "[46]

Even beyond the historical context, the article that gave birth the right to privacy more than a century ago had a human-centric concept of privacy in mind.[47] The right to be

---

[42] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' ").

[43] *Id.* at 195-96.

[44] Amy Gajda, *What If Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage that Led to "The Right to Privacy,"* 2008 MICH. ST. L. REV. 35, 59 (2008). *See also* MELVIN I. UROFSKY, LOUIS D. BRANDEIS: A LIFE 98 (2010). Neil Richards argued that Warren and Brandeis' motivation should be viewed within the context of their elite social status, as they sought to protect the upper class from the unwanted gaze of the lower class. Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1302 (2010).

[45] LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY, 49-50 (2012); Erwin Chemerinsky, *Rediscovering Brandeis Right to Privacy*, 45 BRANDEIS L.J. 643, 644 (2007).

[46] Warren & Brandeis, *supra* note 42, at 195.

[47] Even though the Warren and Brandeis's work is credited for the creation of the legal right of privacy, legal notions regarding privacy originated even before the Warren and Brandeis's article. Some U.S. courts recognized indirect legal protection for personal interests in privacy through the law of confidentiality. *See* Gajda, *supra* note 44, at 1045 (citing Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007)).

let *alone* assumed the need to withdraw from other human beings. All envisioned instances of privacy violations in the article involved the publication of personal information about individuals. Similarly, in all the information flows mentioned in the article, humans communicated information to other humans, either directly or through media technology means.[48] The tort of privacy is intended to protect humans' ability to develop "inviolate" personalities without unwelcome interference from prying eyes and ears of others.[49]

In their outline of the right to privacy, Warren and Brandeis differentiate between written publication and oral publication, assuming that the injury resulting from oral communications would be trivial that the law should not make allowances for it.[50] This difference between oral and written communication lies in the limits of human cognitive abilities to spread information and keep record of it in the absence of writing: without recording technologies, a word of mouth cannot travel too far and is likely to be forgotten quickly. Machine observation is decoupled from human observation only in one statement in the article, which exemplifies more than all how Warren and Brandeis' conceptualization of privacy is construed against the backdrop of human interaction only:

> "If we are correct in this conclusion, the existing law affords a principle which may be invoked to protect *the privacy of the individual* from invasion either by the too enterprising press, the photographer, or *the possessor* of any other modern device for recording or reproducing scenes or sounds (emphasis added)."[51]

Privacy protection is not required against the recording or reproducing of scenes and sounds, but against the *human possessor* of the contained information. Warren and Brandeis' emphasis on the human possessor may be interpreted narrowly to apply only in the context of legal liability. However, devices at that time could not independently produce the privacy harms that Warren and Brandeis outlined in their work. Thus, it is very unlikely that Warren and Brandeis prescribed such a human-machine differentiation only in the context of legal liability. It is more likely that they did not envision any privacy harm that can result in the absence of a human gaze.

Another foundational conception of privacy is Alan Westin's 1967 book Privacy and Freedom. In his work, Westin envisioned privacy as a developing spectrum of involvement with the public sphere: solitude, intimacy, anonymity, and reserve.[52] In the

---

[48] *See, e.g.*,: "The common law secures *to each individual* the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated *to others*" Warren & Brandeis, *supra* note 42, at 198; "A *man* writes a dozen letters *to different people*. No person would be permitted to publish a list of the letters written" *id.* at 201; All of the *publication* cases in pages 207-213; "The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the *personal appearance, sayings, acts, and to personal relations, domestic or otherwise,*" *id.* at 213; " The design of the law must be to protect *those persons with whose affairs the community* has no legitimate concern, from being dragged into an undesirable and *undesired publicity* and to protect all persons, whatsoever; their position or station, from having matters which they may properly prefer to keep private, *made public against their will*." *Id.* at 214-15 (emphasis added).

[49] *Id.* at 205.

[50] *Id.* at 217.

[51] *Id.* at 206.

[52] Alan F. Westin, Privacy and Freedom 31-32 (1967).

most private stage – solitude – the individual is completely isolated from other people,[53] while the next stage – intimacy – allows for involvement with a limited social circle.[54] Next, the individual remains anonymous in the public sphere by avoiding the attention of others,[55] and in the final state the individual prevents others from accessing personal information with the help of self-erected or otherwise imposed barriers to the sharing of information.[56] Westin's spectrum is construed against the backdrop of human observation and judgement. The gradual move from the solitude stage to the reserve stage is measured by the allowed amount of human involvement. Considerations like power dynamics, abuse, and manipulation are not even implied in Westin's spectrum because the most basic metric at the core of the privacy interest is to what extent a human is watching and judging another human. Westin, like Warren and Brandeis, saw the value of privacy in the power it gives individuals to withdraw from others, "that some measure of exemption from full observability be provided for."[57]

b. Human Centric Privacy Torts

Courts and legislators responded to Warren and Brandeis' call to redress privacy harms through the creation of new torts as early as 1903.[58] In 1960, William Prosser, at that time the Reporter for the Second Restatement of Torts, reported more than 300 privacy cases and classified them based on four legally protected interests: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light or "publicity"; and (4) appropriation.[59] Collectively known as "invasion of privacy," these categories by Prosser have quickly won broad acceptance and formed the foundation of the privacy torts of the Restatement (Second) of Torts.[60] These categories represent the interference with the right to be let alone.[61]

When describing the first tort of intrusion upon seclusion Prosser refers to physical intrusion into one's private space and to non-physical intrusion by eavesdropping or peering into a window of a home.[62] The second tort represents the core of the privacy interest envisioned by Warren and Brandeis - public disclosure of (embarrassing) private facts. As Prosser emphasizes, the public disclosure of private fact protects a reputational interest and acts as an extension of defamation with the elimination of the defense of truth.[63] The third

[53] *Id.* at 31.
[54] Id.
[55] *Id.* at 32.
[56] Id.
[57] *Id.* at 58 (quoting Robert Merton, Social Theory and Social Structure 375 (1957)).
[58] Solove, *supra* note 11, at 1432. *See also* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 977, 979 (1964).
[59] Solove, *supra* note 11, at 1432. Prosser, *supra* note 38, at 389.
[60] Solove, *supra* note 11, at 1432. (pointing out that "whether by statute or common law, most states recognize some or all of the privacy torts.")
[61] Prosser, *supra* note 38, at 389.
[62] *Id.* at 390.
[63] *Id.* at 398.

tort involves publicity that places an individual in a false light in the public eye. Here too, the interest protected is reputational, but unlike public disclosure of private facts, which exposes true facts about individuals, the false light act is based on fabricated lies.[64] The fourth and last category protects against the exploitation of attributes of an individual's identity. Prosser explains that the name acts as a symbol of an individual's identity as there is no exclusive right to the use of any name.[65] Unless there is clear identification and association between the information attributed to an individual and that individual no tort of appropriation materializes.[66]

The four privacy torts and the cases reviewed by Prosser all involved a closed privacy circuit with a human observer and a human observed. The harm was accordingly measured against the exposure to other humans and their subsequent judgment.[67]

c. The Fourth Amendment

The human-centric approach to privacy is also reflected in Fourth Amendment case law and scholarly works. In the *Katz* case,[68] the Supreme Court famously moved away from the traditional marriage of the right to privacy and property interests, to testing privacy interests based on subjective and objective expectations of privacy.[69] Post *Katz*, the Supreme Court refused to find that a Fourth Amendment search has occurred if the information was merely collected/processed by a machine without human involvement.[70] In *United States v. Karo*[71] the Supreme Court distinguished between the use of a technology to collect information and the conveyance of this information to the police, referring to the former as a potential privacy violation, as opposed to the latter which is an actual privacy invasion.[72] This line of reasoning continued implicitly in *Kyllo v. United States*.[73] In *Kyllo*, the Supreme Court held that Fourth Amendment protection does not extend to heat waves outside a house, meaning the detection of radiation by a machine is not, by itself, a search. But once the thermal scanner allowed the police to gain information about activity inside the house, this measurement of emanations turned into a search.[74]

---

[64] *Id.* at 398.

[65] *Id.* at 403.

[66] Prosser, *supra* note 38. at 405.

[67] Even though it explicitly rejects the human/nonhuman distinction when it comes to identifying a privacy harm, Ryan Calo's theory of privacy harm captures this intuition well. Calo argues that the privacy harm falls into one of two related categories: subjective harm, which refers to "the perception of unwanted observation," and objective harm, which includes the "unanticipated or coerced use of information concerning a person against that person." M. Ryan Calo, *The Boundaries of Privacy Harm,* 86 IND. L.J. 1131 (2011).

[68] Katz v. United States, 389 U.S. 347 (1967).

[69] *Id.* at 351-52.

[70] Orin S. Kerr, *Searches and Seizure in a Digital World*, 119 HARV. L. REV. 531, 553-54 (2005).

[71] 468 U.S. 705 (1984).

[72] *Id.* at 712.

[73] 533 U.S. 27 (2001).

[74] *Id.* at 35.

Back in 2005, Orin Kerr identified this human-centric approach in Fourth Amendment jurisprudence and scholarship.[75] Using the human-centric logic in the early days of digital searches, Kerr proposes an "exposure-based approach" to interpreting Fourth Amendment searches and argues that a search occurs "when information from or about the data is exposed to possible human observation."[76] Kerr explains that using human exposure to information as a measurement for the search invasiveness accurately transfers physical world notions of searches to the virtual context of computers,[77] reinforces the traditional Fourth Amendment concern with limiting the scope of searches,[78] and is easier to administer than alternative approaches because humans are better in controlling and understanding exposure than controlling and understanding the technical functioning of a computer.[79]

In a later important work, Matthew Tokson argues that "the automated collection of personal data without eventual exposure to a human observer does not constitute a loss of privacy in theory or law."[80] Tokson traces the human-centric approach to early pre-digital conceptions of privacy in the legal literature, but explains that the idea of the human observer remains central to the conception of privacy even in theories developed after the advent of electronic surveillance.[81] Even in theories of privacy that view privacy as control over one's personal information, Tokson claims that concerns about data collection are grounded in the potential for human involvement.[82] In support of this view he cites polls on consumer behavior that are indicative of users' human centric approach to privacy.[83] Tokson also conducted a survey, which was modeled after Christopher Slobogin & Joseph Schumacher's study of the perceived invasiveness of different types of police actions.[84] In his survey, Tokson found participants regarded automated use of their data as intrusive, but less invasive than human use.[85]

Tokson, like myself, uses the distinction between human and automated observation to bolster privacy protection. Specifically, this distinction bears crucial consequences to the application of the Third-Party Doctrine. Under the third party doctrine, Fourth Amendment protection does not apply to information disclosed to a third party and obtained by the

---

[75] Kerr, *supra* note 70, at 549-57.
[76] *Id.* at 551.
[77] *Id.* at 551-52.
[78] *Id.* at 552.
[79] Id.
[80] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 616 (2011). Importantly, Tokson explains that "[i]t is beyond the scope of this Article to advance a particular theory of privacy, or to give a comprehensive account of what should be considered a 'privacy harm..'" *Id.* Rather, this Subpart makes a limited theoretical claim about what does not constitute a loss of privacy. It argues that information disclosed only to an automated system remains 'private' as that word is commonly used and *as it is used in Fourth Amendment law*." *Id.* at 611-12 (emphasis added).
[81] *Id.* at 612.
[82] *Id.* at 614.
[83] *Id.* at 620-21.
[84] Id. at 622-26 (citing Christopher Slobogin & Joseph E. Schumacher, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society", 42 DUKE L.J. 727 (1993)).
[85] *Id.*

government from that party.[86] In Smith v. Maryland, the Court mentioned that the fact that the process was automated, which means that information was "disclosed" to a machine and not to a human third party, was irrelevant to the Fourth Amendment inquiry.[87] As Tokson rightly notes, in an information age, excluding the troves of digital trails users create from the scope of Fourth Amendment protection grants the government unprecedented power to monitor the communications of individuals and organizations.[88] The third party doctrine is predicated on the belief that individuals who choose to divulge information to other people assume the risk that this information may later be shared with the police, therefore waiving any Fourth Amendment expectation of privacy in the information disclosed .[89] By following the simple logic that has traditionally guided our privacy laws and scholarship, Tokson argues that exposure of personal information to automated systems results in no loss of privacy.[90] Thus, the assumption of risk imputed to the sharing individual under the third party doctrine should not apply in the context of automated collection and use, because individuals do not experience a privacy loss and retain reasonable expectations of privacy in that information.

In *Carpenter v. United States*, the Supreme Court delivered an important ruling concerning the third-party doctrine. Carpenter, who was suspected of a number of store robberies, argued that his Fourth Amendment rights were violated when law enforcement acquired records of his cellular location data for the time periods during which the robberies took place.[91] Even though the facts of the case involved a full privacy circuit with humans on both ends,[92] it is fascinating to see how the Court resorts to rhetoric that humanizes technology, yet acknowledges the difference between a human process and an automated one. For example, writing for the majority, Chief Justice Roberts maintains that

> "The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. *Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible.* There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."[93] (emphasis added)

These approaches in Fourth Amendment scholarship and case law not only make intuitive sense but are also better protective of privacy interests on the one hand, and of

---

[86] Tokson, *supra* note 80 at 584.
[87] Smith v. Maryland, 442 U.S. 735, 744 (1979).
[88] Tokson, *supra* note 80, at 585.
[89] United States v. White, 401 U.S. 745, 752 (1971).
[90] Tokson, *supra* note 80, at 586.
[91] Carpenter v. United States, 138 S. Ct. 2206, 2212-13(2018).
[92] As most Fourth Amendment cases are, as the dissent opinion explains in *Carpenter* "Fourth Amendment rights, after all, are personal." *Id.* at 2227.
[93] *Id.* at 2219.

other informational interests on the other hand, than the current approach. In the context of the Fourth Amendment the right to privacy has acted as an instrument of limiting government power. Historically, protecting against unwanted human observation and judgment has been a byproduct of the practical inability to perform humanless government surveillance. But as government surveillance becomes increasingly humanless, the privacy interest is no longer a byproduct. This does not mean that Fourth Amendment protection is a dead letter. Quite the opposite. It means that Fourth Amendment protection can and should focus on its prime objective – to restrict government power, regardless of whether a privacy interest is implicated.

d. Regulation of De-Identified or Encrypted Data

Privacy and security laws in the United States generally do not regulate de-identified and encrypted data. Leaving aside rightful criticism as to the vulnerability of de-identified data,[94] this approach, which is explicit in various privacy and security laws, follows the human-centric view of privacy. If an individual cannot be meaningfully identified by another human, no privacy concern arises. Breach notification laws, the Health Insurance Portability and Accountability Act (HIPAA) regulations, and the California Consumer Privacy Act (CCPA)[95] illustrate the human-centric approach in the context of cybersecurity protection.

Responding to digital threats involving data breaches, states have stepped in to ensure a satisfactory level of cybersecurity protection and accountability to their citizens. The protection has largely taken the form of breach notification statutes.[96] Starting in 2003, state legislators passed laws requiring that breached entities notify users if certain personal information that describes those individuals has been or may have been compromised.[97] All fifty states and U.S. territories include an encryption safe harbor provision in their breach notification statutes. Following the human-centric logic, the encryption safe harbor releases entities from the notification duty if the compromised data was encrypted.[98]

---

[94] *See, e.g.*, Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, PROC. OF THE 29TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY, May 2008, https://ieeexplore.ieee.org/document/4531148; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Boris Lubarsky, *Re-Identification of "Anonymized Data"*, 1 GEO. L. TECH. REV. 202 (2017).

[95] See discussion below infra notes 95-103.

[96] Beth Burgin Waller & Elaine McCafferty: The Necessary Evolution of State Data Breach Notification Laws: Keeping Pace with New Cyber Threats, Quantum Decryption, and the Rapid Expansion of Technology, 79 WASH. & LEE L. REV. 521, 522 (2022)

[97] Emily Matta, Kansans at Risk: Strengthened Data Breach Notification Laws as a Deterrent to Reckless Data Storage, 67 U. KAN. L. REV. 823, 833 (2019). See also David Thaw, The Efficacy of Cybersecurity Regulation, 30 GA. ST. U. L. REV. 287, 297 (2014);Baker & Hostetler LLP, Breach Notification Law Interactive Map, https://www.bakerlaw.com/BreachNotificationLawMap (filter by "encryption safe harbor").

[98] Matta, *supra* note 97, at 834. *See also* James H. Ferguson III, Protecting Personal Data: A Survey of Consumer Protections Throughout North Carolina's Identity Theft Protection Act, 42 CAMPBELL L. REV. 191, 202 (2020); Henry Adams, The Federalist Regulation of Privacy: The Happy Incidents of State Regulatory Activity and Costs of Preemptive Federal Action, 84 MO. L. REV. 1055, 1070 (2019);,), and Scott R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 TEX. L. REV. 85, 159

A similar approach is evident in the Health Insurance Portability and Accountability Act (HIPAA). HIPAA regulates use and disclosure of "protected health information" which is defined as "individually identifiable health information:"[99]

> "Individually identifiable health information is information that ... [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual" and either (a) identifies the individual, or (b) provides a "reasonable basis to believe the information can be used to identify the individual."[100]

Nevertheless, once such protected health information has been sufficiently de-identified, HIPAA's privacy rule protection no longer applies to the use or disclosure of the de-identified information.[101] Under HIPAA, there are two acceptable methods to de-identify protected health information. The first offers a safe harbor following (1) the removal of specific enumerated identifiers from the information and (2) if the covered entity has no actual knowledge that the information could be used (alone or in combination with other information) to identify the information subject.[102] The second method requires an expert rendering the information not individually identifiable and confirming that the risk of re-identification of the information subject is very small.[103]

The California Consumer Privacy Act (CCPA) imposes a wide range of obligations on entities that collect, use, or sell personal information.[104] The CCPA includes a de-identification exception, and defines de-identified information as

> "[I]nformation that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:
> (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
> (2) Has implemented business processes that specifically prohibit reidentification of the information.
> (3) Has implemented business processes to prevent inadvertent release of deidentified information.
> (4) Makes no attempt to reidentify the information."[105]

Like breach notification laws and HIPAA, the CCPA follows the human-centric approach and, while establishing more stringent requirements for a valid de-identification, also places emphasis on the human ends of the privacy circuit.

(2014) (noting that the practice of applying data-breach notification statutes only to already-identified datasets (datasets that include name or other clearly identifying information) is the dominant current approach to state data-breach notification laws).

[99] 45 C.F.R. § 160.103 (2019)

[100] Id.

[101] 45 C.F.R. §§ 164.502(d), 514(a)-(c).

[102] 45 C.F.R. § 164.514(b)(2)(i).

[103] *Id.* § 164.514(b)(1)(i).

[104] Cal. Civ. Code § 1798.100 *et seq.*

[105] Cal. Civ. Code § 1798.140(h).

As this section demonstrates, our privacy norms, laws, and institutions have evolved with a human-centric view of privacy. The human/humanless divide is clearly present throughout the legal history of privacy. The assumption of a human in the loop also explains the turbulence that the privacy discourse experienced with the proliferation of information technologies. While the continuous use of the privacy toolkit to address new informational harms seemed intuitively right at the time, it had resulted in an ever-expanding privacy concept. As the next section explains, overbroad privacy has been failing to address core privacy interests, but equally importantly, it has been diverting from effectively addressing other informational harms.

IV. THE FAILURE OF OVERBROAD PRIVACY

In her book, *Surveillance Capitalism*, Shoshana Zuboff explores a new mutant form of capitalism in which human experience is used as free raw material for translation into behavioral data.[106] Zuboff acknowledges that some of the data is utilized to improve products and services, but the rest is treated as "proprietary behavioral surplus."[107] These data leftovers are used in advanced machine intelligence processes and generate prediction products that anticipate behavior.[108] Zuboff notes that "Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are willing to lay bets on our future behavior."[109]

Privacy scholars, like Zuboff, have long argued that information-driven risks go far beyond individual privacy and bear broad social consequences.[110] Yet, privacy rhetoric has been routinely used to address both individualistic and social implications of information collection and use, pushing the privacy bundle further away from the human element. Over time the term privacy has become not only practically and conceptually overloaded, but also counterintuitive and, as a result, often discredited.

This section is dedicated to showing how the privacy bundle has expanded over time to include humanless surveillance and how that expansion has contributed to privacy's conceptual and strategic failures.

a. Privacy's Conceptual Failure

In her canonical book, "Legislating Privacy," Priscilla Regan grapples with a pressing question: Why has privacy failed so badly as a policy goal?[111] Regan examined privacy lawmaking in three key areas: computerized databases, wiretapping, and polygraph testing. She found that in all three areas, privacy has been failing repeatedly because its

---

[106] Shoshana Zuboff, The Age of Surveillance Capitalism 8 (2019).
[107] *Id.*
[108] Id.
[109] *Id.*
[110] REGAN, *supra* note 5,NISSENBAUM, *supra* note 33.
[111] REGAN, *supra* note 5, at xi-xii.

protection was justified on purely individualistic grounds.[112] In the legal and philosophical literatures privacy was framed as *an individual value* that must back down in the face of what was viewed as more important *societal values*.[113] Even though theoretical underpinnings for a societal view of privacy emerged in the late 1960s-early 1970s, the abstract view that privacy is "an important functional requirement for the effective operation of social structure"[114] failed to influence public policy choices.[115] Regan counteracted those views by calling for a multi-dimensional view of privacy. In her view, privacy offers a "common value," a "public value," and a "collective value."[116] Privacy is a common value because all individuals recognize the importance of some degree of privacy in their lives; a public value because the proper functioning of democratic political systems requires privacy protection of individuals, and a collective value because "technology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy."[117] Similarly, Colin Bennett distinguished between the humanistic and political aspects of privacy.[118] The humanistic value necessitates control over personal information to maintain dignity, autonomy, and respect for the individual, whereas the political value is rooted in the way privacy limits information-based power shifts from the individual to large institutions.[119]

Both Regan and Bennett accurately forecasted that personal information collection would bring about broad societal harms that will only exacerbate over time. Their arguments place crucial emphasis on the shift from the individual value of privacy to the societal, public, common, and political interests that privacy serves. Nevertheless, it is only recently that this view has been significantly acknowledged in public discourse. But even now, when privacy seems to enjoy its golden era, what should be protected under privacy and how protection should be designed is still unclear. The definition of privacy, in accordance with important efforts by privacy scholars to move away from the individualistic approach, has swelled dramatically to embrace all information-related issues. And while Scholars like Regan and Bennett were right to point out that collection of information creates societal risks that extend beyond the individualistic domain the continuous use of the term privacy ironically undermined that important message. The term privacy keeps circling back to individual interests, not because the broader societal concerns are ignored, but because the term privacy intuitively invokes human observation of another human. As human observation becomes the exception rather than the norm, concerns about dramatic loss of privacy in the individualistic sense have lost credibility and consequentially caused all privacy claims to sound overstated and irrelevant: The erosion of human presence has made some privacy claims highly counterintuitive.

---

[112] *Id.* at xi-xii.

[113] *Id.* at xi-xii, 16, 19.

[114] ALAN WESTIN, PRIVACY AND FREEDOM, 58 (1967).

[115] James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 69-70 (2003).

[116] REGAN, *supra* note 5, at 213.

[117] *Id.*

[118] COLIN J. BENNETT, REGULATING PRIVACY 23-33 (1992).

[119] *Id.* at 23, 30.

One example for such counterintuitive application involves the way by which the expansive definition of privacy groups together social implications that are derived from scaled individual harms and social implications that do not originate in individual harms. The privacy bundle includes both individual rights that have collective value and collective values that are affected by individual choice and control. For example, surveillance that results in large-scale chilling of individual speech clashes with essential democratic values like freedom of expression and diversity of opinions.[120] However, social harms can result from collection and use of personal information even if the collection and use do not directly harm individuals but involve their "choice" to authorize sharing of information, such as when a business' dominance in a specific personal information market produces anti-competitive barriers to entry.[121] While violating individual rights that have collective value traditionally involved a human element, harms to collective values that are dependent on (scaled) individual control are relatively new and more often than not, humanless. As such, clustering both under the term privacy, which traditionally involved heavy human presence on both ends, is confusing and counterintuitive.

Furthermore, even while advocating for a broader privacy bundle, many privacy scholars inadvertently reveal their own search for the human in the loop. For example, many privacy scholars view the collection of personal information, regardless of the use, to be harmful.[122] They explain the harm in the uneasy sense that "*someone out there knows something about me.*"[123] This sense of helplessness, which led to Solove's call for moving away from the 1984 rhetoric to The Trial's perceptions of surveillance, invokes broader risks of data collection, but still emphasizes the individualistic, and more important – *human* – notion of privacy.[124]

Refining the definition of privacy to reflect the growing humanless collection and use of personal information is crucial to establishing conceptual clarity. When Solove advocates for abandoning the big brother metaphor in favor of the helplessness perceived in "The Trial" he emphasizes the importance of conceptualization.[125] Solove quotes John Dewey who said, "A problem well put is half-solved," and explained that the way we conceive a problem directly impacts the choice of specific solution routes and the data selection.[126] In Solove's view, which is more than applicable to the argument advanced here, the way we conceptualize a problem has key ramifications for policymaking:

> "I argue that the Big Brother metaphor as well as much of the law that protects privacy emerges from an older paradigm for conceptualizing privacy problems…Privacy law has developed with this paradigm in mind,

---

120 *See* Ruth Gavison, *Privacy & The Limits of Law*, 89 YALE L.J. 421(1980); Julie Cohen, *Privacy, Visibility, Transparency, & Exposure*, 75 U. CHI. L. REV. 181 (2008).

121 Lev-Aretz & Strandburg, *supra* note 23, at 296-306.

122 Helen Nissenbaum, *Deregulating Collection: Must Privacy Give Way to Use Regulation?*, 21 (May 1, 2017) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3092282.

123 Nehf, *supra* note 112, at 70-71.

124 Similar to Solove's argument for moving away from 1984 rhetoric to language of The Trial. Solove, *supra* note 11. *Id.* at 1398.

125 *Id* . at 1399.

126 *Id.*

> and consequently, it has failed to adapt to grapple effectively with the database problem."

As our privacy laws and policies evolved around a human centric notion, it is essential to revisit the current paradigm, which keeps expanding the somewhat narrow human-centric view of privacy and ask whether this expansion is wise conceptually and strategically. As the above discussion illustrates, recognizing the social implications of data collection is imperative, but placing these implications within an inflated privacy bundle is intuitively wrong and has been backfiring for years. As individuals keep looking for the human in the loop whenever the term privacy is in use, the individualistic quality of the privacy interest remains dominantly present. Consequentially, not only information-driven social problems fail to gain significant public support for the entire privacy bundle, but those problems also seem to suffer the same hindrances that narrower individualistic privacy has suffered all along: they are pitted against other social values and asked to step back.

b. Privacy's Strategic Failure

As the above discussion demonstrates, conceptual accuracy stands to support the narrowing of the privacy bundle and exercising precision around informational problems. The current conceptual disarray also yields strategic consequences. The current disorientation around the definition of privacy is exacerbated with more informational risks that move away from a human-centric dynamic. As a result, not only privacy, in the narrower-individualistic sense, loses power with claims like "privacy is dead"[127] and "I've got nothing to hide,"[128] but also privacy, in the broader social sense, is not being properly accounted for. In other words, it is a strategic lose-lose: a loss for privacy in the individualistic sense, and an even greater loss for privacy in the broader social sense. To explain the strategic failure, this section opens with some examples of users' human-centric perceptions of privacy, continues with evidence of lawmakers' human-centric privacy views, and concludes by showing how the privacy terminology promotes privacy whitewashing by industry players.

i. Users' Privacy and the Human Element

The clustering of all informational risks under the term privacy has largely led users to three mental states: activism, helplessness-infused indifference, and true indifference. The activist group, when realizing the potential and actual consequences of data collection, react by attempting to preserve their privacy. Some do it effectively, by withdrawing from social networks, using privacy respecting search engines and browsers, and resorting to

---

[127] Microsystems' CEO Scott McNealy's famous statement that "Privacy is dead, get over it," was just the first of many similar statements over the years. *See* Katherine Noyes, *Scott McNealy on Privacy: You Still Don't Have Any,* PC WORLD June 25, 2015, https://www.pcworld.com/article/2941052/scott-mcnealy-on-privacy-you-still-dont-have-any.html.

[128] *See, e.g.*, Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 748 (2007).

privacy enhancing technologies or obfuscation methods. The helpless group is perfectly described by The Trail's metaphors. In the face of ubiquitous data collection and complex web of uses and flows, which are closely tied to powerful market players, users feel that nothing can give them meaningful control over their information, so they choose to do nothing. And the truly indifferent group that also keeps sharing information, usually explains its indifference in convenience or in the fact they have got nothing to hide. Users' reactions to the Cambridge Analytica scandal showcase how these groups interpret privacy as human-centric, and how this interpretation shapes their attitude towards information-related problems.

Following the Cambridge Analytica scandal, many have forecasted the beginning of Facebook's end. Soon after the story broke a movement to delete users' accounts emerged and the hashtag #DeleteFacebook trended.[129] Users' actual relationships with the social network, however, turned out to be more complex than originally perceived. Nearly seven weeks after the Cambridge Analytica revelations, Reuters and Ipsos published a poll showing that most of Facebook's U.S. users have remained loyal to the social network.[130] A Pew Research Center survey found in September 2018 that 42% of respondents reported to have taken a break from checking the platform for a period of several weeks or more, and 26% said they have deleted the Facebook app from their phone.[131] Nevertheless, in January of the following year, Facebook reported to have 1.52 billion daily active users, which shows a 9% increase from the same period in 2018.[132] Facebook's first 2019 quarter results highlighted what investors and analysts have described as "exceptionally strong" consumer demand.[133] Facebook's second 2020 quarter report shows strong business and user growth even amid the coronavirus pandemic.

---

129 *#DeleteFacebook Trends Amid Cambridge Analytica Scandal*, CBS NEWS, Mar. 21, 2018, https://www.cbsnews.com/news/deletefacebook-trends-amid-cambridge-analytica-scandal/. *See also* Jefferson Graham, *'Happier Without Facebook': Users Who Deleted the Social Network Say They're Not Looking Back*, USA TODAY, Dec. 24, 2018, https://www.usatoday.com/story/tech/talkingtech/2018/12/24/delete-facebook-movement-these-readers-did-and-theyre-still-happy/2406792002/

130 Chris Kahn & David Ingram, *Three-Quarters Facebook Users as Active or More Since Privacy Scandal: Reuters/Ipsos Poll*, REUTERS, May 6, 2018, https://www.reuters.com/article/us-facebook-privacy-poll/three-quarters-facebook-users-as-active-or-more-since-privacy-scandal-reuters-ipsos-poll-idUSKBN1I7081. For poll data see *Reuters Poll Data, Social Media Usage Poll* 05.03.2018, https://fingfx.thomsonreuters.com/gfx/rngs/FACEBOOK-PRIVACY-POLL/010062SJ4QF/2018%20Reuters%20Tracking%20-%20Social%20Media%20Usage%205%203%202018.pdf

131 Andrew Perrin, *Americans are Changing Their Relationship with Facebook*, PEW RESEARCH CENTER, Sept. 5, 2018, https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/. For the survey methodology see *The American Trends Panel Survey Methodology*, PEW RESEARCH CENTER, https://assets.pewresearch.org/wpcontent/uploads/sites/1/2018/09/FT_18.09.05_FacebookPrivacy_MethodologyTopline.pdf.

132 Danielle Abril, *Despite All Its Blunders, Facebook Continues to Attract New Users*, FORTUNE, Jan. 31, 2019, http://fortune.com/2019/01/30/facebook-users-increase-despite-scandals/

133 *Facebook Reports First Quarter 2019 Results*, FACEBOOK INVESTOR RELATIONS, Apr. 24, 2019, https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-First-Quarter-2019-Results/default.aspx; *See also* Jayson Derrick, *Investors Give Facebook's Quarter A Thumbs Up; What Does The Street Think?* , Apr. 25, 2019 https://www.benzinga.com/analyst-ratings/analyst-color/19/04/13596927/investors-give-facebooks-quarter-a-thumbs-up-what-does-the-street-think.

Specifically, the social media giant reported 1.79 billion daily active users worldwide, with 198 million daily active users in North America alone.[134]

Moving from numbers[135] to users' reactions to the Cambridge Analytica fallout further sheds light on the way users understood the nature of the scandal. In June 2018, The Atlantic published a survey pushed out to the magazine's readers on its social media outlets and through its membership program.[136] Note that the demographic of the sample is probably skewed towards educated young professionals who one would expect to be well familiar with the implications of the Cambridge Analytica debacle.[137] When asked whether they were worried about the privacy of their information on social media, the majority of respondents claimed they were either very concerned or somewhat concerned.[138] When asked whether the Cambridge Analytica news changed their behavior on Facebook, nearly 42% responded that it did.[139] 9.6 percent of respondents deactivated or deleted their accounts.[140] But the rest mostly reacted by either being more careful about what they post and/or posting less, and changing their privacy settings.[141] Most of them reported posting less personal information on social media compared to five years ago.[142]

The Atlantic survey is an important testimony to the human-centric nature of privacy in users' perceptions.[143] The participants in the survey were aware of the Cambridge Analytica scandal and likely understood the privacy implications more than the average person. Yet, when changing their behavior, most respondents were attempting to shield themselves from human observation and judgment as opposed to the protecting themselves from the harmful information practices that allowed the scandal to take place. Users self-censored or limited their perceived engagement. It might also be the case that by referring

---

134 Etan Vlessing, *Facebook Tops 2.7 Billion Monthly Active Users in Latest Quarter,* BILLBOARD, July 30, 2020, https://www.billboard.com/articles/business/9427355/facebook-tops-2-7-billion-monthly-active-users-earnings-report.

135 Facebook's engagement numbers reflect only part of the story. Some forms of user engagement are declining for reasons other than privacy concerns. Specifically, younger users think of Facebook as "grandmother's" social network and move to alternative platforms like Facebook-owned Instagram and WhatsApp as well as Snapchat. Nick Statt, *Facebook's US User Base Declined By 15 Million Since 2017, According to Survey*, THE VERGE, MAR. 6, 2019, https://www.theverge.com/2019/3/6/18253274/facebook-users-decline-15-million-people-united-states-privacy-scandals (noting however that "Meanwhile, Instagram is booming"). Engagement numbers are also impacted by other factors such as "the worldwide shelter-in-place and quarantine orders due to the COVID-19 pandemic that have everyone using social networks and staring at screens far more than average." Nick Statt, *Facebook Usage is Surging, But the Company Warns It May Be Temporary,* THE VERGE Apr. 29, 2020, https://www.theverge.com/2020/4/29/21241845/facebook-q1-2020-earnings-coronavirus-covid-19-daily-users-engagement-up.

136 Julie Beck, *People Are Changing the Way They Use Social Media*, THE ATLANTIC, June 7, 2018, https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/.

137 *Id.* (99% of respondents said they were aware of the Cambridge Analytica news).

138 Id.

139 Id.

140 Id.

141 Id.

142 *Id.*

143 Additional surveys are presented in Tokson's work on perceptions of Fourth Amendment privacy. *See* Tokson *supra* note 80, 619-26.

to changing privacy settings, most users referred to adjusting different exposure levels and limiting visibility of the information they share on Facebook. The option to curb exposure, however, is effective only against other users, and not so much against platforms that have unlimited access to user data. Even though the problems highlighted by the Cambridge Analytica case had very little to do with self-doxing or social interactions with others, users still reacted by limiting information sharing with their contacts on the platform. They did not limit the information sharing with Facebook, the same type of information sharing that capacitated the abuse by Cambridge Analytica, because that abuse was portrayed virtually everywhere as a privacy violation. In search of mitigation, users first looked for the human in the loop, and they found it in the form of their Facebook's contacts and friends.

ii. Lawmakers' Privacy Views

The strategic failure of overbroad privacy is further evident in lawmakers' positions and statements around different informational issues in which the privacy issue is marginal at best. The human-centric view of privacy explains why lawmakers struggle to move away from a notice and consent model when it comes to information management. Democratic principles like liberty and autonomy dictate that decisions about an individual's personal information be made by that individual. Notice and consent, at least theoretically, allow users to make informed decision about the costs and benefits of the sharing. The cost-benefit analysis advanced by the notice and consent model is *an individual*, *as opposed to social,* analysis. Individuals consider the costs and benefits of the sharing in individualistic terms, including the privacy cost.[144] As humans increasingly leave the informational loop, individuals sense that their individual privacy is not threatened and agree to share more. Social informational harms, however, materialize even, and in many cases more, in the absence of an individual privacy harm. The marriage of the two under the term privacy is counterintuitive to many lawmakers, who not only use human-centric rhetoric but also devote their efforts to promoting an improved notice and consent model.

Following the Cambridge Analytica scandal Congress called in Mark Zuckerberg, Facebook's founder and CEO, for a hearing during which lawmakers questioned Zuckerberg for hours on how Facebook has handled its user data and countered efforts to subvert democracy.[145] Many of the questions included general calls for adapting privacy protections to contemporary informational challenges.[146] But even those who try to be more

---

[144] Lev-Aretz & Strandburg, *supra* note 23, at 284 (discussing the failures associated with individual decision-making in informational transactions).

[145] Zack Wichter, *2 Days, 10 Hours, 600 Questions: What Happened When Mark Zuckerberg Went to Washington,* N.Y. TIMES, Apr. 12, 2018, https://www.nytimes.com/2018/04/12/technology/mark-zuckerberg-testimony.html.

[146] For example, Senator Chuck Grassley (R-Iowa), the Chairman of the Senate Judiciary committee, stated that "Our policy towards data privacy and security must keep pace with these changes. Data privacy should be tethered to consumer needs and expectations. Now, at a minimum, consumers must have the transparency necessary to make an informed decision about whether to share their data and how it can be used. Consumers ought to have clearer information, not opaque policies and complex click-through consent pages. The tech industry has an obligation to respond to widespread and growing concerns over data privacy and security and to restore the public's trust. The status quo no longer works. Moreover, Congress must determine if and how we need to strengthen privacy standards to ensure transparency and understanding for the billions of consumers who utilize

precise, resorted to the human-centric rhetoric. Senator Bill Nelson (D-FLA) asked to "cut to the chase" and warned that "(i)f you and other social media companies do not get your act in order, none of us are going to have any privacy anymore. That's what we're facing."[147] But when describing the loss of privacy he envisioned, Senator Nelson pointed to "personally identifiable information that, if not kept by the social media — media companies from theft, a value that we have in America, being our personal privacy — we won't have it anymore."[148] Senator Richard J. Durbin (D-ILL) asked Zuckerberg: "would you be comfortable sharing with us the name of the hotel you stayed in last night?" The audience burst into laughter as Zuckerberg answered: "no." Durbin then continued to ask, "If you messaged anybody this week, would you share with us the names of the people you've messaged?" and Zuckerberg replied "Senator, no. I would probably not choose to do that publicly, here." This moment was celebrated as one of the iconic moments of the hearing, as Senator Durbin concluded "I think that may be what this is all about: your right to privacy, the limits of your right to privacy and how much you give away in modern America in the name of, quote, "connecting people around the world."'[149]

Those questions as well as others in the Zuckerberg hearing demonstrated that lawmakers keep looking for a human in the loop. The information collected and used by Facebook for targeted advertising does not pose the same concerns that are posed by disclosing Zuckerberg's lodging information to the world or sharing his text message exchanges. While the former is virtually humanless and produces at scale risks of, *inter alia*, discrimination and manipulation, the latter is all about human observation followed by judgment and potentially safety risks.[150] The grouping together of human privacy violations and humanless surveillance leads to conceptual confusion, and, even worse, drives lawmakers to promote policy changes based on a mixed-up paradigm that is likely to fail in practice.

The Zuckerberg hearings also highlighted that lawmakers continue to rely heavily on the notice and choice model, looking for ways to "ensure transparency and understanding for the billions of consumers."[151] Very little has been said about potential restrictions on how Facebook uses its users' data, even if users agree to have information about them used, for example, for political targeting. The notice and consent approach, which is also dominant in pending privacy bills,[152] is grounded in respect for individual autonomy.

---

these products." *Transcript of Mark Zuckerberg's Senate Hearing,* WASH. POST, Apr. 10, 2018 https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/

147 Id.

148 Id.

149 Id.

150 Gideon Lewis-Kraus, *Facebook and the 'Dead Body' Problem*, N.Y. TIMES, Apr. 24, 2018,https://www.nytimes.com/2018/04/24/magazine/facebook-and-the-dead-body-problem.html.

151 Zuckerberg's Senate Hearing Transcript, *supra* note 146 (statement of Sen. Charles E. Grassley (R-Iowa)).

152 Jonathan M. Gaffney, *Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress*, CONG. RSCH. SERV. Apr. 3, 2020, https://www.hsdl.org/?abstract&did=836400 ("each proposal would create notice and consent requirements for how covered entities would use covered information. Under these requirements, a covered entity would have to notify an individual when it intends to collect or transfer information. The entity would then have to ask the individual for affirmative consent (opt in) or give the individual a chance to opt out of the collection or transfer.")

Individuals should have the power to choose whether they are willing to share certain information and for what purposes. But this emphasis on individual choice, even with restrictions such as data minimization and purpose limitation, does not adequately account for broader information-driven social harms. Such harms, including discrimination, manipulation, and excessive market power, do not receive the appropriate legislative attention as they are often lost in the overbroad privacy bundle.

iii. Silicon Valley and Privacy Whitewashing

The use of privacy as a blanket term is also part of what seems to be a general tendency of resorting to blanket terms in the face of new technological challenges. As this section explains, the use of overbroad terminology has created a fertile ground for whitewashing and conceptual manipulation both in the context of privacy and in neighboring tech policy contexts. The strategic failure, in this sense, is double sided: Legislative attempts fail and lack precision, and in the resulting regulatory vacuum industry players harness the vagueness of broad terminology to whitewash destructive choices.

As discussed above, when informational risks started gaining recognition, privacy seems to be the best available concept to address those risks, even though it exhibited many conceptual and strategic challenges. Similar clustering has been used in the context of big data analytics and machine learning, with calls for "data justice,"[153] and the Fairness, Accountability and Transparency in Machine Learning [FATML] movement.[154]

Another bundle term that is becoming growingly popular is "AI ethics" (also referred to as data ethics or tech ethics). Recent years have made it clear that AI applications raise troubling ethical issues around error, bias, their black box nature, and more. And while ethical concerns around technology have been, just like privacy, discussed for years, recent scandals have highlighted them and they began trending in the public eye.[155] As a result, AI

---

[153] *See, e.g.*, Lina Dencik, Arne Hintz & Jonathan Cable, *Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism*, BIG DATA AND SOC'Y, Dec. 2016, at 1,, https://journals.sagepub.com/doi/full/10.1177/2053951716679678; Jeffrey Alan Johnson, *From Open Data to Information Justice*, 16 ETHICS AND INFO. TECH. 263 (2014); Linnet Taylor, *What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally*, BIG DATA AND SOC'Y, Dec. 2017, at 1,, https://journals.sagepub.com/doi/full/10.1177/2053951717736335.

[154] FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY IN MACHINE LEARNING, http://www.fatml.org/ (last visited May 19, 2022). Also *see, e.g.*, Emily M. Bender & Batya Friedman, *Data Statements for Natural Language Processing: Toward Mitigating System Bias and Enabling Better Science*, 6 TRANSACTIONS OF THE ASS'N FOR COMPUTATIONAL LINGUISTICS 587 (2018), https://direct.mit.edu/tacl/article/doi/10.1162/tacl_a_00041/43452/Data-Statements-for-Natural-Language-Processing; Willie Boag et al., *Modeling Mistrust in End-of-Life Care* (2018), https://arxiv.org/abs/1807.00124; Cynthia Dwork & Christina Ilvento, *Group Fairness Under Composition*, FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY IN MACHINE LEARNING (2018), https://www.fatml.org/media/documents/group_fairness_under_composition.pdf; Nitin Madnani et al., *Building Better Open-Source Tools to Support Fairness in Automated Scoring,* 2017 PROCS. OF THE FIRST WORKSHOP ON ETHICS IN NAT. LANGUAGE PROCESSING 41 (2017), https://www.aclweb.org/anthology/papers/W/W17/W17-1605/.

[155] Daniel Susser, *Ethics Alone Can't Fix Big Tech*, SLATE, Apr. 17, 2019, , https://slate.com/technology/2019/04/ethics-board-google-ai.html.

ethics is now everywhere: In April 2019 an independent expert group set by the European Commission published Ethics Guidelines for Trustworthy AI.[156] The tech sector displays an extensive embrace of AI ethics principles, with the publicized founding of ethics boards and ethics charters, as well as sponsorship of AI ethics research.[157] Academic investments are also being made in developing and offering ethics courses for computer and information science students,[158] establishing research centers like Stanford's Institute for Human-Centered Artificial Intelligence[159] and participating in public-private initiatives like the Partnership on AI.[160]

Nevertheless, many have criticized the current AI ethics wave for being a display of self-regulation to avoid regulation.[161] The AI ethics initiatives, including those of the European Union are said to be broad, ineffective, and not offering true ethics but merely ethics-washing.[162] When referring to how the AI ethics trend not only failed in mitigating the risks it is set to address but also in some cases ends up exacerbating them, Daniel Susser writes:

> "*Desperate for anything to rein in otherwise indiscriminate technological development, we have ignored the different roles our theoretical and practical tools are designed to play. With no coherent strategy for coordinating them, none succeed*."[163]

Privacy shares a similar story. In addition to triggering many counterintuitive uses of the term, overbroad privacy has been used for whitewashing. Joseph Turow, who studies privacy perceptions of online and offline consumers, found that when users see the phrase "privacy policies" most of them assume their information is kept private.[164] This knowledge gap, Turow explains, is a direct result of the misleading label of privacy policies that businesses are happy to preserve because it embodies blissful ambiguity.[165]

---

[156] Eur. Comm'n, Ethics Guidelines for Trustworthy AI, (2019), https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

[157] James Vincent, *The Problem With AI Ethics*, THE VERGE Apr. 3, 2019, https://www.theverge.com/2019/4/3/18293410/ai-artificial-intelligence-ethics-boards-charters-problem-big-tech.

[158] Natasha Singer, *Tech's Ethical 'Dark Side': Harvard, Stanford and Others Want to Address It*, N.Y. TIMES Feb. 12, 2018, https://www.nytimes.com/2018/02/12/business/computer-science-ethics-courses.html.

[159] STAN. UNIV. HUMAN-CENTERED A.I., https://hai.stanford.edu/ (last visited May 19, 2022).

[160] Susser, *supra* note 155.

[161] *Id. See also* Ben Wagner, Ethics as an Escape from Regulation: From "Ethics-Washing" to Ethics-Shopping?, in BEING PROFILED, COGITAS ERGO SUM: 10 YEARS OF PROFILING THE EUROPEAN CITIZEN 84 (Emre Bayamlioğlu, Irina Baraliuc, Liisa Janssens & Mireille Hildebrandt eds., 2018).

[162] Susser, *supra* note 155. *See also* Yochai Benkler, *Don't Let Industry Write the Rules for AI*, NATURE, May 1, 2019, https://www.nature.com/articles/d41586-019-01413-1.

[163] Susser, *supra* note 155.

[164] Joseph Turow, *Americans & Online Privacy: The System is Broken* (2003), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1411&context=asc_papers; Joseph Turow et al., *Open to Exploitation: America's Shoppers Online and Offline* (2005), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers; Joseph Turow, *Let's Retire the Phrase 'Privacy Policy'*, N.Y. TIMES Aug. 20, 2018, https://www.nytimes.com/2018/08/20/opinion/20Turow.html [hereinafter *Let's Retire the Phrase*].

[165] Turow, Let's Retire the Phrase, supra note 164.

Furthermore, as policy discussions have centered around privacy policies and appropriate disclosure, other important informational issues that are laundered through the privacy policy have been sidetracked.[166] As the above examples show, precision is key in avoiding whitewashing and advancing effective protections against informational risks. The first step in the difficult mission of bringing privacy into a state of precision must be with acknowledging an accurate the intuitive gravity of human presence in privacy.

V. DECOUPLING PRIVACY FROM HUMANLESS INFORMATIONAL HARMS

The prior discussion examines the shift from human-centric privacy to humanless privacy and the inflated privacy concept it has created over time. The treatment of all informational harms as privacy violations stands in the way of protecting against the risks it is set to address. The association of informational harms with human gaze results in an indifference to humanless surveillance.

This section spells out the application of a narrower, human-centric approach to privacy. It starts by explaining the basic definition of privacy in human-centric terms, leaving humanless surveillance outside the scope of privacy to be treated under a broader data protection paradigm. Then this section lists the immediate benefits of the proposed conceptual shift, namely moving away from the notice and consent model to legal mechanisms that address informational harms beyond the individual, identifying tools to scrutinize the legitimacy of humanless information flows, and incentivizing different kinds of strategies for political mobilization.

a. No Privacy Circuit – No Privacy Violation

Our legal institutions and policy choices have evolved around the notion of human-centric privacy. This Article advocates for making privacy about humans again, by requiring a closed privacy circuit as a prerequisite to establishing privacy violation. Under this theory, a closed human circuit includes a human watching and a human watched. A humanless informational chain could cause many informational harms, but until a human enters the loop, privacy violation is not one of them. When a human watches a data point, the privacy risk increases, but it does not harm privacy because one-sided human watching is not a closed privacy circuit. Here too, the dynamics may, and probably do, give rise to informational risks like bias, error, financial fraud, discrimination, and more, but it does not give rise to a privacy concern unless human observation is expected down the line.

When an information flow involves a human watcher and a human watched, the circuit is closed, and a privacy interest may be materializing. The fact that a privacy interest may be materializing does not mean that it does materialize, and it does not mean that a privacy violation necessarily ensued. Humans regularly watch humans and in many of these interactions no privacy violation comes about. Does an individual's encounter with a

[166] *See, e.g.*, Alexandra Chouldechova & Max G'Sell, *Fairer and More Accurate, But for Whom?* (2017), https://arxiv.org/abs/1707.00046.

stranger on the train constitute privacy violation? Well, it depends. When the stranger merely looks at the individual as they step into the train, perhaps assessing the individual but within acceptable social boundaries, it is likely that no privacy violation occurred. However, when that stranger listens in on the phone calls the individual makes on the train, looks at clues on the individual's belonging, and proceeds with extensive online research to identify the individual and learn about his or her life – a privacy violation likely took place.[167] As pointed out above, the key to distinguishing between instances of privacy violations and instances of acceptable social interaction is assessing the contextual norm using the contextual integrity theory.[168]

The contextual integrity theory offers a framework for modeling intuitive judgments when information flows undergo radical changes as exemplified by the above scenario.[169] A practice would be violating contextual integrity when it transgresses context-relative informational norms.[170] Those norms are understood through four identifiers of the information flow: the relevant contexts;[171] the actors, including the sender and receiver of the information and the information subject;[172] the attributes, which refer to "the kind and degree of knowledge;"[173] and the transmission principles that set the conditions under which information should transfer.[174] When one of the identifiers of the information flow changes, the change is flagged as a prima facie breach of contextual integrity.[175] Next, moral and political factors implicated by the changes in flow are considered, followed by an evaluation of these factors in the specific context, and concluding with a final judgment as to the compatibility of the information practice with contextual integrity principles.[176]

To put differently, unlike privacy, the contextual integrity theory offers an excellent toolkit to scrutinize informational concerns. While it, too, maintains some ties to the privacy concept, it is designed in broader terms that move away from the human-centric intuitions that the concept privacy currently invokes. The contextual integrity paradigm also explicitly recognizes illegitimate flows that do not involve privacy violations, such as when the information flowing is about corporations and non-living.[177] It is comprehensive, inclusive, and amenable to changing norms. Privacy acts as one of many informational concerns under the contextual integrity paradigm but in no way does privacy equal contextual integrity.

---

[167] Kate Klonick, *A 'Creepy' Assignment: Pay Attention to What Strangers Reveal in Public*, N.Y. TIMES, Mar. 8, 2019, https://www.nytimes.com/2019/03/08/opinion/google-privacy.html.

[168] NISSENBAUM, *supra* note 33, at 180.

[169] *Id.* at 181.

[170] Id.

[171] *Id.* at 141.

[172] *Id.* at 141-43.

[173] *Id.* at 143-45.

[174] *Id.* at 145-47.

[175] *Id.* at 150.

[176] *Id.* at 158-66.

[177] For a practical application of the theory in the context of corporate data, see Yan Shvartzshnaider, Zvonimir Pavlinovic, Ananth Balashankar, Thomas Wies, Lakshminarayanan Subramanian, Helen Nissenbaum & Prateek Mittal, *VACCINE: Using Contextual Integrity for Data Leakage Detection*, WWW '19: THE WORLD WIDE WEB CONFERENCE May 13, 2019, https://doi.org/10.1145/3308558.3313655.

Contextual integrity is broader and encompasses what privacy is currently en route to enclose – all information-related concerns.

b. Consent and Human Privacy Myopia

Aside from several sectoral laws, information use is governed exclusively by a contractual notice and consent model. Privacy self-management, as Daniel Solove puts it, means that individuals have the right to decide for themselves whether the costs of information collection and use outweigh the benefits or vice versa.[178] And once individuals agree, meaning that they believe the benefits outweigh the costs, their consent legitimizes nearly any legal form of information collection and use.[179] The view that notice and consent "is being tasked with doing work beyond its capabilities"[180] is quite established by now, with more and more scholars and activists pointing out the weaknesses of the current model.[181] However, many of them, Solove included, struggle to define the cases in which individual consent should be overridden.[182] Lawmakers have similarly gone astray when attempting to exercise paternalistic approach and instead focused on adding friction points at which individuals would hopefully get to better evaluate the costs and benefits of the informational transaction. Such friction points exist in current federal privacy bills – most of which include opt-in consent mechanisms.[183]

It is easy to see the heart of this conflict: consent in the current consent model is fictional, but paternalism is worse as it explicitly deprives people of their freedom to make consensual choices about their data.[184] The understanding that privacy interests only comes into play with human observation over humans, shows that setting up rules to replace notice and consent is in fact not paternalistic. Solove notes that "the correct choices regarding privacy and data use are not always clear" and gives two examples to show that paternalism can interfere with entirely legitimate privacy choices: a bulimic person sharing her experiences and medical information with the world via social media, and people who are interested in sharing data for targeted marketing.[185] The human-centric model of privacy treats those two examples differently. In the first example, the individual sharing her

---

178 Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880 (2013).
179 Id.
180 *Id.* at 1880.
181 *See, e.g.*, James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1181-82 (2009); Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, 89 GEO. L.J. 2029, 2041 (2001) (showing how current consent models harm users' privacy rights without offering sufficient information or true control), and Lev-Aretz & Strandburg, *supra* note 23, at 285 ("Even to the extent information is provided in privacy policies, users face extremely high transaction costs of obtaining, reading, and understanding those notices. Privacy policies are often vague, too complicated to be understood by an average user, and liable to be changed at any time, sometimes without notice.")
182 Solove, *supra* note 1782, at 1894-98.
183 Gaffney, *supra* note 152.
184 Solove, *supra* note 178, at 1881-82. *But see* Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 755-57 (1999) (exploring restrictions on some forms of individual liberty to mitigate the erosion of societal expectations of privacy).
185 Solove, *supra* note 178, at 1895-96.

experiences on social media implicates a clear privacy interest as she is being watched by other people. It makes perfect sense to allow her to manage observation and judgment of her actions. Her information flow is legitimate and is made with respect to context – she chooses what to share and with whom.[186] In the second example, no human element is involved and thus no privacy interest. The sharing of personal information for marketing then must be evaluated against additional informational problems such as discrimination, bias, and security, but privacy is out of the list of immediate concerns.

The oversight around privacy's human-centric nature caused or at the very least significantly contributed to the legal neutrality around the merits of a particular form of data collection or use.[187] Individual choice has trumped over other central values because the human-centric paradigm justifies individual control over personal information. The failure of the consent model, however, aptly shows that many of the challenges that information technology presents cannot be addressed through individual control.[188] Furthermore, those challenges should not be left to individual choice that is affected by behavioral and cognitive limitations, among which privacy myopia has been especially singled out. Michael Froomkin, who coined the term, uses it to describe consumers' undervaluing of their personal information: valuing it at its marginal value to themselves as opposed to at its much higher value in the market.[189] Consumers also fail to value the loss of privacy from each isolated instance of data collection or may wrongly prioritize short-term gains over long-term cost.[190]

The argument advanced in this article calls attention to an additional type of privacy myopia: Because individuals are accustomed to thinking about privacy as involving human presence, when asked to waive their privacy they measure the privacy harm only in terms of *human* observation and judgment. Upon realizing that no human is watching, individuals waive their privacy altogether, disregarding warnings about massive loss of privacy and resulting social harms. The human-centric tunnel vision that is endemic to individual decisions around data collection and use further highlights the inadequacy of the consent model in humanless collection and use.

c. Same Problems – Different, More Effective Legal Tools

Refocusing legal attention away from the human centric model would create new avenues for advocacy around legislative and judicial change. Keeping privacy human-centric would drive political mobilization that is more precise and thus more effective in forcing legal reforms to adapt accordingly. Moving away from overbroad privacy would

---

[186] Note that the fact there is no privacy violation doesn't mean that other informational risks do not exist. At this point, the contextual integrity model would take us to the next step – to look outside the narrow individual interest into social and ethical considerations.

[187] *Id.* at 1902-03.

[188] 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 (2020).

[189] Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1501-1505 (2000).

[190] Id.

also result in the repurpose of existing legal tools as well as the creation of new legal and policy tools to address the changing technological landscape.

Privacy torts, for example, represent human-centric privacy in its strongest form. It is thus not surprising that privacy torts have failed to effectively address broader informational problems and offer meaningful recourse in cases involving humanless tracking. The Ninth Circuit has already signaled that a humanless privacy violation could be successfully countered by the claim that the information has not been disclosed "to the public,"

> "Perhaps Facebook could have made a better argument, which is that *there's a difference between publicizing your sensitive information for actual human beings to scrutinize (like, in a newspaper) and allowing your information to be added to the vast sea of "big data" that computers rather than humans analyze* for the purpose of sending targeted advertising on behalf of companies. Perhaps there is an argument that the former is the "public disclosure" of information within the meaning of California law while the latter is not."[191]

As such, privacy torts should remain narrow, follow the human-centric focus and consequentially propel precise definition and targeting of informational issues outside privacy.

Antitrust law, however, has been commonly brought up as an answer to big tech power and potentially unfair competition, including in the context of dominance in personal information markets and erecting barriers to entry. Information markets represent a singular case in this context. As Professor Katherine Strandburg and myself have argued elsewhere, markets for personal information-based products and services erect distinctive natural barriers to entry because of the unique qualities of personal information, including its association with specific individuals, its non-linear aggregation and, its collection as a by-product of offering goods or services. [192] The interplay between misaligned demand signals in personal information markets and incentive distortions associated with variation in the extent to which suppliers can appropriate returns from innovative activities jointly affect the innovation portfolio and its social value.[193] Moving away from human-centric privacy into antitrust regulation, a move we gradually witness,[194] can truly address problems that

---

[191] *In re* Facebook, Inc., Consumer Privacy User Profile Litig., 402 F. SUPP. 3D 767, 796 (N.D. Cal. 2019).

[192] Lev-Aretz & Strandburg, *supra* note 23, at 302-303.

[193] *Id.* at 273-75.

[194] Two key pieces of legislation have been recently introduced to rein in the power of major tech players: S.2992- the American Innovation and Choice Online Act and S.2710 - Open App Markets Act. Under the American Innovation and Choice Online Act, large online platforms would not be able to favor their own products or services, disadvantage competitors, or discriminate against companies using their platforms in ways that would harm competition on that platform. American Innovation and Choice Online Act, S. 2992, 117th Cong. (2021). The act would also forbid dominant platforms from interfering with other services or using another company's data to compete against it. *Id.* Under the Open App Markets Act, dominant app stores with more than 50 million US users would be prohibited from engaging in certain anti-competitive behaviors, such as "unreasonably" promoting their own apps in search results and limiting developers' ability to contact prospective customers directly. Open App Markets Act, S.2710, 117th Cong. (2021).

originate in personal information collection but impact far beyond it in contexts of market dominance, anticompetitive behavior, and more.

Another example for an overdue refocusing of informational harms away from human-centric privacy is election laws. The Cambridge-Analytica scandal illustrated the risks of covertly eliminating individual choice. Cambridge Analytica threatened autonomy and choice at the cornerstone of the democratic process, which should be addressed under election laws. While most of the legal discussion around Cambridge Analytica centered on foreign interference with US election, the ability to effortlessly manipulate voter choice has been a significant part of the problem, which can and should be addressed through election laws.[195] Grassroots lobbying by tech platforms that uses personal information to target their users with political ads further exacerbates some of those concerns. Most of these efforts are not disclosed as they are not considered "lobbying" and are outside the scope of federal public disclosure rules.[196] Even though personal information is involved in the targeting, this is a classic example of humanless surveillance that does not trigger privacy interests, but instead crucially involves broader social and deliberative democracy risks.

Overbroad privacy rhetoric has similarly been distractive is the context of discrimination laws. The potential for disparate impact is already built into the use of big data because of the common use of proxies and is further exacerbated by automation.[197] An algorithm can pick up on the fact that a certain individual has specific ethnic or demographic characters and deliver this information to another algorithm that targets job postings or housing ads at them. This example is not hypothetical: In September 2019, the ACLU has filed charges with the Equal Employment Opportunity Commission against Facebook and a number of other companies for targeting certain ads for jobs to younger male Facebook users.[198] The ACLU has reported that these charges joined other litigation alleging race discrimination in job, housing, and credit ads and age discrimination in job ads.[199] While this discrimination is powered by the intensive collection of personal information, and while it requires the use of this information for highly personalized marketing, this discrimination is often completed without any human in the loop. The risks of replicating, perpetuating, and even exacerbating biases are there regardless, and keeping privacy human-centric refocuses efforts on addressing the illegal discrimination causing them, and not the ancillary potential privacy harms.

---

[195] *See, e.g.*, Samir Sheth, *Super Pacs, Personal Data, and Campaign Finance Loopholes*, 105 VA. L. REV. 655 (2019) (exploring how federal election laws and regulations have failed to keep pace with the collection and sophisticated use of data by *campaigns and other political organizations and calling* to regulate personal data like any other campaign asset); Samuel Woolley & Nicholas Monaco, *Amplify the Party, Suppress the Opposition: Social Media, Bots, and Electoral Fraud*, 4 GEO. L. TECH. REV. 447 (2020) (discussing the legal implications for the use of political bots and other forms of computational propaganda during elections).

[196] *See* Abbey Stemler, *Platform Advocacy and the Threat to Deliberative Democracy*, 78 MD. L. REV. 105 (2018); see Tech News Briefing, Bills to Rein In Big Tech Face Fierce Lobbying Ahead of Key Meeting, WALL ST. J., Jan. 20, 2022, https://www.wsj.com/podcasts/tech-news-briefing/bills-to-rein-in-big-tech-face-fierce-lobbying-ahead-of-key-meeting/758744fe-2ffe-4ce7-9196-93e53a22a92d.

[197] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 691-92 (2016).

[198] Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU, Mar. 19, 2019, https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping.

[199] Id.

II. VI. CONCLUSION

Privacy is fighting an endless battle. Even in the face of publicized examples of harmful and abusive use of personal information, the privacy paradox keeps making puzzling appearances, and privacy policymaking is largely ineffective. This Article steps into a years-long theorizing by offering an additional, intuitive yet overlooked reason for privacy's ongoing failure: Privacy law has evolved with a human-centric approach, assuming the presence of a human observer and a human observed. Information technologies, however, changed this very basic privacy dynamic by facilitating humanless information flows, in which the human observer turned into an algorithm and the human observed transforms into data points. The familiar and useful privacy rhetoric has naturally extended to describe informational harms resulting from new uses of personal information, including humanless flows. As a result, privacy became a loaded bundle term that covers all possible information-related problems.

This expansion, which was the only reasonable reaction to emerging information technologies at the time, has been harmful for information technology policymaking as the human-centric view kept creeping in with the use of the term privacy. This Article argues that privacy should be viewed as a human-centric value, which conforms to the way it has evolved in the law and to social norms as reflected by the perceptions of users and lawmakers. Information technology challenges should be precisely identified, in accordance with the problems they bring up, and not indirectly through privacy violations. Once informational issues are successfully divorced from privacy and defined in light of existing social norms, available legal tools can be used or repurposed to address them, and new legal tools can be effectively devised.