OKLAHOMA CITY UNIVERSITY
LAW REVIEW

VOLUME 49 WINTER 2024 NUMBER 2

ARTICLE

THE REGULATORY LESSON FROM THE FEDERAL TRADE COMMISSION'S STAFF REPORT, "A LOOK BEHIND THE SCREENS": LET THE TECH LOBBYISTS WIN

Collin R. Walke[*]

INTRODUCTION

In September 2024, the Federal Trade Commission ("FTC") issued a staff report entitled *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services*[1] (the "Report"). The Report was the product of orders to file special reports under Section

[*] Collin Walke is a partner at Hall Estill and leads their Cybersecurity and Data Privacy Practice Group. Collin served in the Oklahoma House of Representatives from 2016-2022. He earned his B.A. in Philosophy from Oklahoma State University, his J.D., *magna cum laude*, from Oklahoma City University School of Law, and is a graduate of Harvard's Business Analytics Program. He is also a ForHumanity certified AI auditor.

1. FED. TRADE COMM'N, A LOOK BEHIND THE SCREENS: EXAMINING THE DATA PRACTICES OF SOCIAL MEDIA AND VIDEO STREAMING SERVICES (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf [https://perma.cc/EP5A-ST7U].

6(b) of the FTC Act[2] issued to "nine of the largest social media and video streaming services—Amazon, Facebook, YouTube, Twitter, Snap, ByteDance, Discord, Reddit, and WhatsApp."[3] Specifically, the orders sought, "information concerning the privacy policies, procedures, and practices of Social Media and Video Streaming Service providers, [i]ncluding the method and manner in which they collect, use, store, and disclose Personal Information about consumers and their devices."[4] The Report recommended that Congress urgently enact comprehensive "privacy legislation that limits surveillance and grants consumers data rights"[5] and asserted that "[l]egislation and regulation are badly needed" with regard to algorithms, data analytics, and AI ("AAA Systems").[6] In short, legislators and regulators must act, the Report warned, because "self-regulation is failing."[7]

As a former legislator who passed one of the strictest data privacy bills in the country[8] out of a state house by a veto-proof bipartisan supermajority, I absolutely agree with the Report. Self-regulation is failing.[9] However, the Report actually proves the lobbyists who fought against Oklahoma and other states' comprehensive data privacy legislation

2. 15 U.S.C. § 41 *et seq.*; 15 U.S.C. § 46(b) (explaining that the Commission shall have the power "[t]o require, by general or special orders, persons, partnerships, and corporations, engaged in or whose business affects commerce, excepting banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, and common carriers subject to the Act to regulate commerce, or any class of them, or any of them, respectively, to file with the Commission in such form as the Commission may prescribe annual or special, or both annual and special, reports or answers in writing to specific questions, furnishing to the Commission such information as it may require as to the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals of the respective persons, partnerships, and corporations filing such reports or answers in writing. Such reports and answers shall be made under oath, or otherwise, as the Commission may prescribe, and shall be filed with the Commission within such reasonable period as the Commission may prescribe, unless additional time be granted in any case by the Commission").

3. *See* FED. TRADE COMM'N, *supra* note 1, at i.

4. *Id.* at 1.

5. *Id.* at 80 (footnote omitted).

6. *Id.* at 83.

7. *Id.*

8. H.R. 1602, 58th Leg., Reg. Sess. (Okla. 2021).

9. *See, e.g.*, ROGER MCNAMEE, ZUCKED: WAKING UP TO THE FACEBOOK CATASTROPHE (2019); *see* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

correct:[10] No amount of legislation or regulation is going to fix the problems America (and the world) will face in the 21st century as a result of surveillance capitalism[11] and AAA Systems.[12] For once, the market, not the law, should be the arbiter of both the collection and commodification of data, as well as the development and deployment of AAA Systems.

The real regulatory lesson to be drawn from the Report is not that there should be more legislation and regulations, but rather, there should be less—a lot less. This Article asserts that there should be but one regulatory requirement for technologies participating in the surveillance capitalism and AAA Systems markets:[13] Surveillance Warning[14] disclosures.

Surveillance Warning disclosures would be standardized similar to nutrition labels on manufactured food products. No longer would consumers have to guess at what data is collected, how it is used, and with whom it is shared. Rather, consumers would know up front if a company surreptitiously collected, for example, health care data from third parties

---

10. *See, e.g.*, Alfred Ng, *The man quietly rewriting American privacy law*, POLITICO (Sept. 18, 2024, 5:00 AM), https://www.politico.com/news/2024/09/17/andrew-kingman-data-privacy-lobbying-00179630; Monique Priestley, *Big Tech Tried to Kill My State's Privacy Bill. Here's What I Learned*, TECHPOLICY.PRESS (May 31, 2024), https://www.techpolicy.press/big-tech-tried-to-kill-my-states-privacy-bill-heres-what-i-learned/ [https://perma.cc/F8PA-8UEV]; Ben Felder, *Data privacy bill passed with wide House support appears dead in the Senate,* THE FRONTIER (Mar. 31, 2021), https://www.readfrontier.org/stories/data-privacy-bill-passed-with-wide-house-support-appears-dead-in-the-senate/ [https://perma.cc/QW9W-SJ6R].

11. For purposes of this note, "surveillance capitalism" means "the unilateral claiming of private human experience as free raw material for translation into behavioral data." John Laidler, *High tech is watching you*, THE HARV. GAZETTE (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ [https://perma.cc/RG86-8JFG].

12. I want to be abundantly clear: I do not actually agree with the argument put forth in this Article. As a former legislator, I am unfortunately confident that somewhere this Article will be cited as though I actually support the argument. However, because I firmly believe that data privacy and AAA Systems legislation need to be re-thought from the ground up, in order to effectively justify regulating tech in a meaningful way the contrary argument must be steel-manned. This is my attempt at that. I do, however, fully endorse the notion of Surveillance Warnings in addition to other regulations.

13. Insofar as this Article is a thought experiment to try and understand the extent of regulation actually necessary to prevent the ails identified by the Report, I am not creating any nuances between developers, manufacturers, deployers, covered entities, business associates, or other operative categories such as controllers or processors.

14. The author does not know the origin of the idea of "surveillance warnings," but was introduced to the concept through the work of data privacy researcher Jeff Jockisch, co-founder of ObscureIQ.

or other undisclosed sources. With this knowledge, the consumer could then be capable of making an informed decision of whether to engage with that company. Plus, the moniker, "Surveillance Warning," is far more accurate given that the Report shows in practice the responsibility to protect privacy is on the consumer, not the company.[15]

Aside from dictating how companies can and cannot collect and use personal data, most data privacy laws also provide data subject access rights ("DSARs"), such as the right of a consumer to request a company copy, edit, or delete the consumer's data.[16] DSARs are seen as part of the solution to the problem of data privacy because they arguably give consumers rights to their data that they would not otherwise have.[17] However, because companies fail to properly manage and account for data, DSARs are empty shibboleths. There simply is no way for a consumer to confirm all of the data a company may have on them or that the company carried out the consumer's request.

At bottom, Surveillance Warning disclosures are not only more efficient at protecting consumers, they are also the *only* practical way to regulate surveillance capitalism and AAA Systems. Section I of this Article addresses the rise in consumer understanding of the risks and benefits of surveillance capitalism and AAA Systems, lending credence to the belief that in a free country where individuals may choose to participate in surveillance capitalism or engage with AAA Systems, individuals will make "good" decisions without the need for governmental regulation. Section II addresses the Report and provides the justification for why governmental regulation is practically impossible and DSARs lack any real meaning. Finally, Section III sets forth the specific policy recommendations for Surveillance Warnings derived from Section II.

---

15. *See* discussion *infra* Section III.

16. *See, e.g.*, *California Consumer Privacy Act (CCPA)*, OFF. OF THE ATT'Y GEN., CAL. DEP'T OF JUST. (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa [https://perma.cc/FRY9-8UQF] (specifying DSAR rights such as the right to know, delete, opt-out, correct, or limit).

17. This author personally experienced the power of DSAR rights. After reading an essay on data privacy, I submitted a DSAR to a data broker. The data broker responded that since I did not live in a jurisdiction with data privacy legislation, they would not disclose what information they held on me.

SECTION I. WE HAVE FAITH IN JURIES, WHY NOT CONSUMERS?

We trust citizens to determine whether a defendant should be put to death and whether a company should be forced to pay punitive damages. We have enough faith in our fellow citizens that we allow them to choose who governs us. So why do legislators and regulators not trust citizens to choose how to participate in surveillance capitalism and AAA Systems?

Historically, it could have been said that consumers were unaware they were being surveilled and that what they were seeing or reading was the product of an AAA System. But for at least a decade,[18] warnings of surveillance capitalism have been constant, and while AI is far more nascent, consumers are becoming more aware of AI's potential risks and harms and changing their behavior accordingly. For example, a Pew Research Center analysis found that in 2021 approximately 18% of adults felt "[m]ore **excited** than concerned" about AI, 45% were "[e]qually excited and concerned," and only 37% were "[m]ore **concerned** than excited."[19] Just two years later, only 10% of adults were "[m]ore **excited** than concerned" and 52% of adults were "[m]ore **concerned** than excited."[20] In other words, even though there are essentially no laws governing AI, consumers are naturally becoming aware of the problems posed by AI and appropriately increasing their concern.

Consumers are also concerned that they do not know what companies are doing with their data, and they do not believe they have much control over their data.[21] Sadly, consumers are not alone: The companies surveyed for the Report "collected so much data *that in response to the Commission's questions, they often could not even identify all the data points they collected or all of the third parties they shared that data*

18. Professor Shoshana Zuboff coined the term "surveillance capitalism" in 2014. *See* John Laidler, *High tech is watching you*, THE HARV. GAZETTE (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ [https://perma.cc/J852-7H8H].

19. Michelle Faverio & Alec Tyson, *What the data says about Americans' views of artificial intelligence*, PEW RSCH. CTR. (Nov. 21, 2023), https://www.pewresearch.org/short-reads/2023/11/21/what-the-data-says-about-americans-views-of-artificial-intelligence/ [https://perma.cc/EY53-5AW5].

20. *Id.*

21. *See, e.g.*, Colleen McClain et al., *How Americans View Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ [https://perma.cc/FT22-LBMC].

with."[22] The inability to actually locate consumer data and account for its use and transfer proves DSARs are empty gestures. If the large companies identified in the Report cannot identify the information necessary to comply with governmental orders, what hope does a consumer have with a DSAR? Moreover, what hope does a consumer have if they submit a DSAR to a smaller company with fewer resources than those identified in the Report? DSAR rights are mere window dressing—much like many of the state-level "comprehensive" data privacy laws.[23]

As the Law of the Horse proves,[24] governments need not pass specialized legislation dealing with data or AAA Systems in order to protect consumers. The common law on copyright and its use in AI software, along with a litany of other novel-use cases involving existing law and 21st century technology,[25] have been or are on their way to being decided. Individuals whose information has been stored negligently or used improperly still have potential claims for relief.[26] Simply because data and AAA Systems are new technologies does not mean that new remedies must be created. Rather, consumers simply need to be informed.

SECTION II. THE REPORT'S FINDINGS.

At first glance, the Report simply confirms what has been public knowledge for some time: Major technology companies are exploiting and manipulating consumers and their data in exchange for money and without much governmental oversight.[27] However, it is worth examining the

22. FED. TRADE COMM'N, *supra* note 1, at i-ii (emphasis added).

23. *See* FED. TRADE COMM'N, *supra* note 1, at 15 n.101 (citing Caitriona Fitzgerald et al., *The State of Privacy: How state "privacy" laws fail to protect privacy and what they can do better*, ELEC. PRIV. INFO. CTR. 725 (Feb. 2024), https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf [https://perma.cc/KW87-DWX9]).

24. K.N. Llewellyn, *Across Sales on Horseback*, 52 HARV. L. REV. 725 (1939) (asserting the argument that simply because a new technology has been developed does not mean that entire new areas of law must be created).

25. *See, e.g.*, Thomson Reuters Enter. Centre GmbH v. Ross Intell. Inc., 694 F. Supp. 3d 467 (D. Del. 2023); *see also* Microsoft Corp. v. IPA Techs. Inc., 2022 WL 989403 (Fed. Cir. 2022); Zhang v. Google LLC, 5:24-cv-02531-EJD (N.D. Ca. Apr. 26, 2024).

26. *See, e.g.*, Johnathan Stempel, *23andMe settles data breach lawsuit for $30 million*, REUTERS (Sept. 13, 2024, 4:56 PM), https://www.reuters.com/technology/cybersecurity/23andme-settles-data-breach-lawsuit-30-million-2024-09-13/.

27. *See* FED. TRADE COMM'N, *supra* note 1, at 15 n.97 (citing FED. TRAD COMM'N,

Report's findings in detail because they shed light on why a Surveillance Warning would work better than any current or proposed regulation pertaining to surveillance capitalism or AAA Systems.

A. SURVEILLANCE CAPITALISTS WILL NOT COMPLY WITH THE FTC, WHY WOULD THEY COMPLY WITH YOU?

The Report specifically addressed the "tech industry's monetization of personal data" and how it "has created a market for commercial surveillance, especially via social media and video streaming services, with inadequate guardrails to protect consumers."[28] According to the Report, policymakers must address the *incentive structure* that has allowed the tech industry to perpetuate problems such as "indiscriminate data collection [and] hyper-granular targeting."[29] The root of that incentive structure is money (hence the very term "surveillance *capitalism*"). Since "data is the new oil,"[30] a prohibition on the commodification of data seems as unlikely as a prohibition on the commodification of oil. Therefore, if the root of the incentive structure cannot be addressed without forcing companies out of business, the question is begged: What can be done?

This question becomes more vexing when one looks at how the companies responded to the Commission's inquiries regarding data sharing practices. They "lacked clear explanations or specificity regarding the exact use cases for sharing with [other entities]."[31] According to the Commission's staff, the "lack of transparency could indicate an inability or unwillingness to account for *the extent of those practices because*

PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/2YPY-8AK8]); *see also* Ng, *supra* note 10.

28. FED. TRADE COMM'N, *supra* note 1, at i.

29. *Id.* at ii. The author personally agrees with the Report on this point in light of Charlie Munger's adage, "Show me the incentive, and I will show you the outcome."

30. Nisha Talagala, *Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires*, FORBES (Mar. 2, 2022, 05:48 PM), https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/#:~:text=Generally%20credited%20to%20mathematician%20Clive,it%20cannot%20really%20be%20used [https://perma.cc/W4FF-TRKE].

31. FED. TRADE COMM'N, *supra* note 1, at 25-26 (footnote omitted).

consumers' data was shared so broadly."[32] What is clear, however, is that if a tech company is unwilling to respond to inquiries from the FTC, under threat of an enforcement action,[33] the average consumer likely has no hope of getting an accurate accounting of data held, used, and transferred. Consumers merely have the *appearance* of control.

Worse yet, surveillance capitalism and data exploitation are not limited to adult data. The Report found that "*no Companies* reported having sharing practices *that treat the information collected from a user known to be aged thirteen to seventeen differently from an adult's information*."[34] "*Only a few* Companies reported engaging in *different* sharing practices with-respect to Personal Information *collected from users under thirteen years of age*."[35] Given that we know children's geolocation data has been shared with data brokers,[36] the sad but true reality proven by the Report is that in cyberspace, a child is no different than an adult.[37]

Since surveillance capitalists and AAA Systems are treating adult and children's data the same, why do data privacy laws make distinctions? Clearly, the distinctions do not matter. Similarly, many privacy laws make distinctions between sensitive data and "normal" personally identifiable information ("PII"). In the 21st century, all PII is "sensitive" given the ability of AAA Systems to infer sensitive information from non-sensitive data.[38] Thus, the Report bolsters the argument that existent data privacy laws cannot be adequately policed, and even if they could, they are written with such antiquated language that new technologies permit exploitations of loopholes.

---

32. *Id.* at 26 (emphasis added).
33. *Id.* at ii.
34. *Id.* at 26 (emphasis added).
35. *Id.* at n.137 (emphasis added).
36. Jon Keegan & Alfred Ng, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users*, THE MARKUP (Dec. 6, 2021, 8:00 AM), https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user [https://perma.cc/XEC6-UANM] (noting "[t]he Markup has learned, however, that the app is selling data on kids' and families' whereabouts to approximately a dozen data brokers who have sold data to virtually anyone who wants to buy it").
37. *See generally* JONATHAN HAIDT, THE ANXIOUS GENERATION: HOW THE GREAT REWIRING OF CHILDHOOD IS CAUSING AN EPIDEMIC OF MENTAL ILLNESS (2024).
38. *See, e.g.*, FED. TRADE COMM'N, *supra* note 1, at 69.

B. AAA SYSTEMS: SURVEILLANCE CAPITALISM'S TOOLS OF THE TRADE.

All of the companies identified in the Report utilized AAA Systems.[39] Unsurprisingly, "[m]ost of the Companies derived revenue from their application of Algorithms, Data Analytics, or AI to Personal Information, whether directly or indirectly."[40] What makes this fact utterly terrifying is that many other companies across the country will be utilizing AAA Systems for purposes other than to make money, like hiring decisions, and those uses are not generally regulated.[41] For example, according to the consulting group Gartner, 34% of human resource professionals said in January 2024 that they were exploring potential use cases and opportunities for generative AI "[*d*]*espite* data privacy, bias[,] and ethical concerns."[42]

Stanford's *Artificial Intelligence Index Report 2024* describes AI as "increasingly ubiquitous."[43] AI's ubiquity also creates a barrier to regulatory enforcement actions, if for no other reason than the resources of any governmental agency are limited. Are already beleaguered privacy enforcement agencies also expected to oversee and enforce AAA Systems regulations? Private rights of action are generally precluded by existing state-level data privacy laws. And so, there is simply no way to comprehensively, and equitably, govern surveillance capitalism and AAA Systems within existing frameworks.

The existence of AI itself creates the inevitable problem of inferences from nominal or limited personal data. As referenced in the Report, "[s]ome researchers have argued that, even when companies offer consumers choices about data collection, the companies may still use big

---

39. *Id.* at 49.

40. *Id.* at 50.

41. One notable exception is New York City's Local Law 144 that "prohibits employers and employment agencies from using an automated employment decision tool (AEDT) in New York City unless they ensure a bias audit was done and provide required notices." *Automated Employment Decision Tools: Frequently Asked Questions*, NYC DEP'T OF CONSUMER & WORKER PROT., https://www.nyc.gov/assets/dca/downloads/pdf/about/DCWP-AEDT-FAQ.pdf [https://perma.cc/8RC8-JQJ8].

42. *AI in HR: The Ultimate Guide to Implementing AI in Your HR Organization*, GARTNER, https://www.gartner.com/en/human-resources/topics/artificial-intelligence-in-hr (last visited Nov. 4, 2024).

43. *Artificial Intelligence Index Report 2024*, STANFORD 3 (2024), https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_AI-Index-Report-2024_Chapter9.pdf [https://perma.cc/4TND-CSRM].

data to draw inferences about consumers who choose to restrict the collection of their data."[44] Consequently, so long as any relatable data exists, there is a decent chance that when analyzed on its own or in conjunction with other data sets, insightful inferences can and will be drawn, irrespective of a consumer's opt-out preferences.

If the record-setting private equity investment into OpenAI is any indication,[45] the use of AI is only going to increase, along with the mass harvesting of data to feed AI. And so, what is the point of even attempting to limit data collection?

The two crystal-clear lessons from the Report are (1) that surveillance capitalism has been and will continue to march forward undeterred irrespective of regulation or governmental threats and (2) AAA Systems are unstoppable economic forces. Given these two lessons, what type of regulation would address both the incentive of capitalism and actually protect consumers? A disclosure regulation.

SECTION III. YOUR "SURVEILLANCE WARNING!": THE ONLY THING NECESSARY FOR AN EFFICIENT, FREE, AND ACCOUNTABLE MARKET.

In *R.J. Reynolds Tobacco Co. v. Food & Drug Administration*, the Fifth Circuit affirmed the constitutionality of legislation mandating that "cigarette packages . . . include 'color graphics depicting the negative health consequences of smoking to accompany the [updated] label statements.'"[46] The ability to require warning labels of "purely factual information" is the linchpin for actually solving the 21st century problems of surveillance capitalism and AAA Systems, as proven by Surgeon General Dr. Vivek Murthy's call for similar authority to place "a surgeon

44. FED. TRADE COMM'N, *supra* note 1, at 61 n.243 (quoting FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (FTC REPORT) 11 (Jan. 2016), https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report [https://perma.cc/87HU-L9EF]).

45. *See* Kate Clark, *OpenAI Asks Investors to Fork Over $250 Million*, THE INFO. (Sept. 19, 2024), https://www.theinformation.com/articles/openai-asks-investors-to-fork-over-250-million (explaining that OpenAI may be soon be valued at $150 billion).

46. 96 F.4th 863, 867 (5th Cir. 2024) (alteration in original) (quoting 15 U.S.C. § 1333(d)).

general's warning label on social media platforms" because of the mental health harms for adolescents.[47]

What would a Surveillance Warning include? Well, in short, in order to fulfill the fictitious concept of a rational consumer, the Surveillance Warning would have to disclose, granularly, the data collected by the company, the uses of the data by specified category, and the disclosure of data by specified category: just like ingredient labels require disclosures of all ingredients and nutritional content.

The granular requirement for types of data collected by the company and with whom it is shared is necessary because otherwise consumers can be duped by misleading broad categories. Understanding the specific data a company collects about a consumer, how it uses that information, and with whom it shares that data allows the consumer to choose whether to engage with that company. Currently, most privacy policies are written in legalese, and no one takes the time to read them.[48] A Surveillance Warning would be simple, standardized, and capable of being understood by anyone who can buy groceries.

Think of the downstream consequences of a Surveillance Warning: First, it would put the world on notice as to what information a company collects, how it uses that information, and with whom that information is shared. By requiring specified categories of disclosures, companies required to post Surveillance Warnings would not have the discretion to choose their own categories, unlike many state-level privacy laws which give discretion to companies on the terms of their privacy policies.[49] This public notice acts as an accountability measure for the company. If a consumer learns that his or her health care information was included in a data breach of a social media company, and the social media company did not disclose that it collected health care information in its Surveillance

47. Vivek H. Murthy, *Surgeon General: Why I'm Calling for a Warning Label on Social Media Platforms*, THE N.Y. TIMES (June 17, 2024), https://www.nytimes.com/2024/06/17/opinion/social-media-health-warning.html.

48. *See, e.g.*, Brooke Auxier et al., *Americans' attitudes and experiences with privacy policies and laws*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/ [https://perma.cc/YKB3-HBJG] (noting that only 13% of adults "sometimes" read privacy policies).

49. *See, e.g.*, TEX. BUS. & COM. CODE § 521.053(j) (2023) (reflecting generically, that "categories" of personal data are to be specified in a privacy notice, without identifying what those categories are); *see also* UTAH CODE ANN. § 13-61-301 (2023) (specifying that "types" of data processed be disclosed without specifying the "types").

Warning,[50] then the plaintiff would have an automatic consumer fraud case.[51] This same public notice also provides consumers with enough knowledge to decide whether to engage with a company.

Second, the very name, "Surveillance Warning," suggests the correct psychological connotation, as opposed to "Privacy Policy." The Report makes it clear that while companies may have policies and procedures in place with regard to the collection and handling of consumers' data, they certainly do not abide by them.[52] This means the onus is on the consumer, not the company, to protect "privacy." If the onus is on the consumer, then a company's policy is irrelevant. What is relevant, however, is the consumers' knowledge *about the company's data practices* in order to make an informed decision as to whether to do business with the company.

And finally, enforceability would be feasible. Instead of attempting to address thousands of DSAR complaints regarding non-compliant companies because private rights of action are prohibited, regulatory enforcement agencies could easily and readily audit the Surveillance Warning disclosures against actual practice. In other words, the role of the enforcement agency becomes that of enforcing regulations against non-compliant corporations, as opposed to a representative of the consumer. The consumer's redress would exist within existing causes of action.

In the future, it may come to be that personal data is governed by traditional property rights,[53] whether for the purposes of taxation[54] or legal redress. But for now, and the foreseeable future, it is clear that technology companies will continue to participate in the surveillance capitalism and AAA Systems markets with, essentially, unfettered discretion. Given that fact, and an attitude of *realpolitik*, the only option is to arm the consumer with the necessary information to make an informed decision.

---

50. One would assume that a specified category would include "health information."

51. Of course, to make this truly effective, legislation prohibiting or narrowing the use of arbitration clauses would have to be enacted.

52. *See* FED. TRADE COMM'N, *supra* note 1, at i, 31.

53. For example, in Oklahoma, a patient who uploads health data to the State's health information exchange "retains a *property right* in the information or data, but grants to the other participants or subscribers a nonexclusive license to retrieve and use that information or data under relevant state or federal privacy laws, rules, regulations, or policies." OKLA. STAT. tit. 63, § 1-133(E) (2024) (emphasis added). Taken to its logical conclusion, such a statutory recognition of property rights in data would mean that if health data was misappropriated, a claim for conversion would exist.

54. *See, e.g.*, S.B. S2012, 2023 Leg., Reg. Sess., (N.Y. 2023) (proposing a data tax).

CONCLUSION

The world is changing rapidly and exponentially through surveillance capitalism and AAA Systems, and the Report is a reminder that there is little the government can do about it. However, there is something consumers can do: choose. Those companies that operate on full disclosure and publicly declare that they do not share or sell your data or otherwise use it for nefarious purposes will be the market winners. Those companies not operating on full disclosure will be found out, and when they are, either consumers or the government will actually have the ability to seek redress.