

---

**From:** Rick Brandt [REDACTED]  
**Sent:** Friday, September 9, 2022 1:14 PM  
**To:** regulations@coppa.ca.gov  
**Subject:** CPPA Public Comment  
**Attachments:** CPPA Public Comment - Opt Out.docx

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender [REDACTED]

Hello,

Thanks for the opportunity to make a comment on this important issue. I may be late, but I think there is a point to be made that has merit and should be heard and considered.

Thanks!!

Sincerely,

*Rick Brandt*

The Real Estate Office of Rick Brandt  
[REDACTED]

CPPA Public Comment – **Automatic Opt Out** – The only real protection.

While I am not a fully informed person regarding privacy laws and practices, I have been alive on the planet for 68 years and therefore have some experience with the institutions that gather, sort, use and sell our personal data – usually without our direct knowledge or permission.

I appreciate the government's efforts to protect its citizens. However, the government's efforts do not solve this problem for its citizens. The idea that a person must opt out of this system does not protect that person's information. No one should have to opt out.

If the government really wants to protect its people, the government should automatically opt every person out. If a person wants their information shared, sold, and distributed they should have to opt in.

Think of it. How many people have the time or desire to read the privacy policy of every single company they interact with. The privacy policies are written in legalese, hard to understand, long, and I would suppose that no one reads them. We all just click or sign so we can finish the business we are there to conduct. The privacy policy is there to protect the company – not the individual. Opting out is often, if not always, a separate task that is not easy to complete.

No one has the time and energy to go around to every company they do business with and opt out. It is ridiculous to think that an option for opting out will protect all people, especially those who need protection the most.

If the rule of law is changed to where an individual is automatically opted out, think of all the paperwork that will be saved and the millions of trees and lawyers fees that will be available for a higher and better purpose. I think that is where we all want to aspire to. Not to the dismal task of opting out to dozens of companies that use our information for their profit.

**Please go all the way to protect individuals and opt everyone out automatically.** That way we are all protected.

Thank you.

---

**From:** Travis Frazier [REDACTED]  
**Sent:** Wednesday, October 19, 2022 11:35 AM  
**To:** [REDACTED]  
**Subject:** Letter on Consent Agenda and Controversial Issues  
**Attachments:** FINAL Joint Ad Trade Letter - CPPA Consent Agenda and Controversial Issues.pdf  
**Importance:** High

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please see attached a letter from the following trade associations regarding the California Privacy Protection Agency's potential consideration of regulations under an abridged "consent agenda" process: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the American Advertising Federation, the Network Advertising Initiative, and the Digital Advertising Alliance. We appreciate your consideration of this letter.

Regards,  
Travis Frazier

Travis Frazier  
Manager, Government Relations | [Association of National Advertisers \(ANA\)](#)

P: [REDACTED]  
2020 K Street, NW, Suite 660, Washington, DC 20006

The ANA drives growth for you, your brand, our industry, and humanity. Learn how at [ana.net/membership](https://ana.net/membership).

October 19, 2022

Chairperson Jennifer M. Urban  
California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

Board Member Chris Thompson  
California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

Board Member Lydia de la Torre  
California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

Board Member Vinhcent Le  
California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

Board Member Alastair Mactaggart  
California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

Executive Director Ashkan Soltani  
California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

**RE: Joint Ad Trade Comments on the CPPA’s Proposed Consent Agenda to Resolve “Non-Controversial” Issues in the CPRA Rulemaking Process**

Dear California Privacy Protection Agency Board Members and Executive Director Ashkan Soltani:

On behalf of the advertising industry, we respectfully urge the California Privacy Protection Agency (“CPPA” or “Agency”) to decline to consider or approve certain controversial regulatory provisions through a “consent agenda” process to expedite the proposed regulations implementing the California Privacy Rights Act of 2020 (“CPRA”). During the CPPA’s September 23 meeting, the Agency expressed interest in placing certain regulatory provisions on a consent agenda for “non-controversial” issues. Shortly thereafter, the Agency published modified proposed regulations to implement the CPRA.<sup>1</sup> There are several issues in the modified proposed regulations that are controversial and unsettled, and therefore should not qualify for any potential consent agenda. Specifically, the following two areas are particularly in need of further discussion and consideration, as they were not addressed by the modifications to the proposed regulations and remain controversial:

- I. Proposed regulations related to opt-out preference signals are missing statutorily mandated safeguards; and
- II. Consumer notice should fulfill the CPRA’s “necessary and proportionate” requirements rather than tying “necessary and proportionate” processing requirements to “average” or “reasonable” consumer expectations.

As the nation’s leading advertising and marketing trade associations, we collectively represent thousands of companies across the country and in California. These companies range

---

<sup>1</sup> CPPA, *Modified Text of Proposed Regulations*, located [here](#).

from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product (“GDP”) in 2020.<sup>2</sup> Our group has more than a decade’s worth of hands-on experience relating to matters involving consumer privacy and controls. We and the companies we represent, many of whom do substantial business in California, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies. We have participated in every proceeding under this CPRA rulemaking, including filing comments in response to the initial draft of proposed regulations. We welcome the opportunity to continue to engage with you to develop regulations to implement the CPRA.

### **I. The Issue of Opt-Out Preference Signals Is Unfit for a Potential Consent Agenda Given Outstanding and Unaddressed Statutorily Required Safeguards**

As the current proposed regulations do not address important statutory safeguards for opt-out preference signals that the CPRA requires, the issue of opt-out preference signals remains controversial and should not be summarily settled via consent agenda consideration. Under the CPRA, the Agency *must* promulgate specific rules to define the scope and form of opt-out preference signals. Specifically, the regulations must “define the requirements and technical specifications for an opt-out preference signal . . . The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should” ensure the signal meets several safeguards: (1) avoids unfairly disadvantaging certain businesses or business models over others in the ecosystem, (2) is clearly described; (3) clearly represents a consumer’s intent and does not employ defaults that presuppose such intent; (4) does not conflict with commonly-used privacy settings consumers may employ; (5) provides a mechanism for consumers to consent to sales or sharing without affecting their preferences with respect to other businesses; and (6) provides granular opt-out options for consumers.<sup>3</sup>

The statute requires CPRA implementing regulations to include such safeguards while “considering the legitimate operational interests of businesses.”<sup>4</sup> However, such technical specifications and safeguards appear nowhere in the current proposed regulations.<sup>5</sup> If the Agency has not resolved where it stands on these statutorily mandated details or made them available for review by interested parties, the issue of opt-out preference signals cannot fairly be considered undisputed or proper for a consent agenda.

The lack of clarity about opt-out preference signals is further exacerbated by a possible truncated window between finalized CPRA implementing regulations and their enforcement date. The CPRA tasks the Agency with finalizing the regulations implementing the law by July 1, 2022, but unfortunately this deadline passed without the Agency issuing final regulations.<sup>6</sup> Yet,

---

<sup>2</sup> John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located [here](#) (hereinafter, “Deighton & Kornfeld 2021”).

<sup>3</sup> Cal. Civ. Code § 1798.185(a)(19)(A) (effective Jan. 1, 2023).

<sup>4</sup> *Id.* at § 1798.185(a)(19)(C).

<sup>5</sup> *See, e.g.*, Cal. Code Regs. tit. 11, § 7025 (proposed).

<sup>6</sup> Cal. Civ. Code § 1798.185(d) (effective Jan. 1, 2023).

enforcement of the CPRA regulations could begin on July 1, 2023.<sup>7</sup> Such an enforcement timeline would grant businesses less than the statutorily intended one-year period to bring themselves into compliance with new regulatory provisions, including provisions on the novel and technically complex subject of opt-out preference signals. The lingering ambiguity surrounding these signals, coupled with a potentially shortened enforcement window, highlights the importance of the statute’s intent that the Agency first promulgate proposed regulations that address all statutorily required terms before mandating that businesses comply.

## **II. The Proposed Regulations Overlook the CPRA’s Recognition of Consumer Notice as a Valid Basis for Data Use, Presenting a Significant Dispute**

The CPRA sets out permissible business purposes for data use *and expressly* states personal information may be used for “other notified purposes.”<sup>8</sup> Despite this statutory text, the proposed regulations introduce an “average” or “reasonable” consumer expectation standard that would make consumer notice obsolete under the statute.<sup>9</sup> The disharmony between the statutory text of the CPRA and well-established consumer privacy principles and what the proposed rules set forth underscores the importance of addressing this issue completely in regular order and not via a consent agenda. The issue deserves a thorough discussion of the benefits of permitting businesses’ data use consistent with their notices to consumers, as well as an explanation of the Agency’s perceived authority to contravene a standard stated clearly in the text of the CPRA itself.

## **III. Conclusion**

We and our members strongly support protecting consumer choice and privacy and preserving responsible data use by commercial businesses operating in California. Given the discussion during the Agency’s September 23 meeting, we urge you to refrain from considering the matters we have mentioned above during any condensed consent agenda process. We will continue to raise these and other critical points in future comments to the CPPA so they may hopefully help to facilitate the CCPA’s rulemaking proceedings. Again, we thank you for the opportunity to participate in the CPRA rulemaking process.

\* \* \*

---

<sup>7</sup> *Id.*

<sup>8</sup> “A business’s collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, *or for another disclosed purpose* that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.” *Id.* at §§ 1798.100(c), 140(e).

<sup>9</sup> The proposed regulations would require “a business’s collection, use, retention, and/or sharing” of personal information to be “reasonably necessary and proportionate to achieve... the purpose(s) for which the personal information was collected or processed... [or] another disclosed purpose that is compatible with the context in which the personal information was collected...” Cal. Code Regs. tit. 11, § 7002(a) (proposed). Both permitted uses of personal information require a consideration of average or “reasonable” consumer expectations. *Id.* at §§ 7002(b); (c)(1).

Thank you in advance for consideration of this letter.

Sincerely,

Christopher Oswald  
EVP, Government Relations  
Association of National Advertisers  
[REDACTED]

Alison Pepper  
Executive Vice President, Government Relations  
American Association of Advertising Agencies, 4A's  
[REDACTED]

David LeDuc  
Vice President, Public Policy  
Network Advertising Initiative  
[REDACTED]

Lartease Tiffith  
Executive Vice President for Public Policy  
Interactive Advertising Bureau  
[REDACTED]

Clark Rector  
Executive VP-Government Affairs  
American Advertising Federation  
[REDACTED]

Lou Mastria, CIPP, CISSP  
Executive Director  
Digital Advertising Alliance  
[REDACTED]

CC: Mike Signorelli, Venable LLP  
Allie Monticollo, Venable LLP

---

**From:** Julie Jensen [REDACTED]  
**Sent:** Tuesday, October 25, 2022 8:19 PM  
**To:** [REDACTED]  
**Cc:** Regulations  
**Subject:** Proofpoint and Rapid7 Follow-up to Public Comments on the California Consumer Privacy Act Regulations – Request for Meeting  
**Attachments:** Proofpoint+\_Rapid7  
\_-\_Follow\_up\_to\_Public\_Comments\_on\_California\_Consumer\_Privacy\_Act\_Regulations.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Soublet,

Please receive the attached follow-up letter in response to the public comments submitted by Proofpoint and Rapid7.

We thank you for your consideration and look forward to your response.

Sincerely,

**Julie Jensen**

Senior Corporate Counsel, Product

Mobile: [REDACTED]

**proofpoint.**

This email is confidential and was prepared by a member of Proofpoint's legal department. It contains advice of counsel and may constitute privileged communication and/or attorney work product. If you are not the intended recipient, please delete immediately and contact the sender.

**FOLLOW UP LETTER IN RESPONSE TO COMMENTS TO CALIFORNIA PRIVACY PROTECTION AGENCY**

October 20, 2022

California Privacy Protection Agency  
ATTN: Brian Soublet  
2101 Arena Blvd.  
Sacramento, CA 95834

**Re: Comments on Title 11(6)(1): California Consumer Privacy Act Regulations – Request for Meeting**

Dear Mr. Soublet,

In response to the call for public comments pertaining to Title 11(6)(1): California Consumer Privacy Act Regulation, Proofpoint, Inc. and Rapid7 submitted a joint letter addressing three sections of the draft CCPA regulations:

- First, we addressed Section 7014, which provides guidance on notice obligations regarding a consumer's right to limit the use of their sensitive personal information, and proposed clarifying modifications to ensure the regulations remain consistent with Section 7027(l)(2) and (l)(3) and do not inadvertently negatively impact security services that offer the type of data protection encouraged and required by the CCPA.
- Second, we addressed Section 7050, where we proposed the addition of anti-fraud prevention and response language so that service providers in the security space can adequately assist businesses with taking reasonable precautions to protect consumer personal information from security breaches.
- Third, we addressed Section 7051 and proposed the addition of anti-fraud exemption language to allow businesses to adequately protect their systems and the customer and consumer information maintained in those systems.

As cybersecurity companies dedicated to helping organizations protect against advanced cybersecurity threats and compliance risks, we believe that strong cybersecurity is essential for consumer protection, and it is critical to ensure cybersecurity activities are permitted to make proportionate use of personal information to manage security risks and incidents. By incorporating our proposed additional language, the Agency has the opportunity to ensure California companies and their consumers remain adequately protected against malicious cyber-attacks and security risks while simultaneously working to ensure consumer privacy protections.

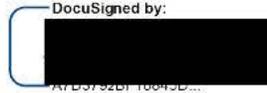
To help ensure that cybersecurity companies such as Proofpoint and Rapid7 are able to continue protecting the businesses and consumers of California, we request an in-person or virtual meeting to further discuss our proposed clarifications and additions to the draft regulations.

We thank you for your consideration and look forward to discussing these matters with you directly.

Sincerely,



**Michael Yang**  
Senior Vice President and  
General Counsel  
Proofpoint, Inc.

DocuSigned by:  


**Raisa Litmanovich**  
Senior Vice President and  
General Counsel  
Rapid7, Inc.

---

**From:** [REDACTED] <[REDACTED]>  
**Sent:** Thursday, October 27, 2022 9:41 AM  
**To:** Regulations  
**Subject:** Important Comments Concerning The Consumer Privacy Rights Act

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender [REDACTED]

With regard to the upcoming Board meeting, we would like to provide the following comments that we consider are important factors that would both strengthen the Act and close potential loop holes in the text as currently written. They are as follows:

1. With regard to the consumer's opportunity to opt-out of the sale and sharing of personal information and do so conforming with the requirements set forth in section 7025 to have their data protected, the current text states that a Business must place this opt-out signal on the home page of their web site. However, it is largely the case that consumers using search engines do so to follow a particular topic and that often this topic is **not** on the home page of a Business web site. In other words, the consumer would not see the opt-out signal as their point of entry to the site.

We suggest that the text is amended to having the opt-out signal present on all pages of a Business web site to ensure consumers have that right available to them irrespective of where they first engage with that site. Doing so would also ensure Businesses can't by-pass this important aspect of the regulations .

2. With regard to consumer data, the terms used throughout the text such as "Do not sell" and "Do not share" are clear and obvious in their meaning and regulatory intent. However the term "Do not use" again seen throughout the text is **confusing and open to interpretation** as to exactly what this entails.

We suggest that "the term "Do not use" is define clearly throughout the text as to its meaning and activities that are covered by it.

We hope and trust you will find these comments helpful and thank you in anticipation of your consideration.

Sincerely,

Pat Whelan



p: [REDACTED]  
w: [www.adtoniq.io](http://www.adtoniq.io)

---

**From:** info@CPPA <info@cpga.ca.gov>  
**Sent:** Thursday, October 27, 2022 11:28 AM  
**To:** [REDACTED] <[REDACTED]>  
**Subject:** Re: Comments Timeline Concerning The Consumer Privacy Rights Act

Thank you for your inquiry.

You may refer to the Frequently Asked Questions on our website to review the process for rulemaking, including the timing of the notice and comment periods: comment: [https://cppa.ca.gov/faq#faq\\_regs\\_2](https://cppa.ca.gov/faq#faq_regs_2)



## Frequently Asked Questions (FAQs) - California Privacy Protection Agency (CPPA)

California Privacy Protection Agency (CPPA)

[cppa.ca.gov](https://cppa.ca.gov)



## Frequently Asked Questions (FAQs) - California Privacy Protection Agency (CPPA)

California Privacy Protection Agency (CPPA)

[cppa.ca.gov](https://cppa.ca.gov)

---

**From:** [REDACTED] <[REDACTED]>

**Sent:** Thursday, October 27, 2022 3:08 PM

**To:** info@CPPA <[info@cppa.ca.gov](mailto:info@cppa.ca.gov)>

**Subject:** Comments Timeline Concerning The Consumer Privacy Rights Act

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

I would be grateful if you would provide me a timeline for comment submission to the Board for their consideration. We have what we consider two important factors that the would both strengthen the Act and close potential loop holes in the text as currently written.

I appreciate your response in due course.

Sincerely,

Pat Whelan



p: [REDACTED] | e: [REDACTED]  
w: [www.adtoniq.io](http://www.adtoniq.io)

---

**From:** Nate Haderlie <[REDACTED]>  
**Sent:** Tuesday, November 1, 2022 11:54 AM  
**To:** Soltani, Ashkan <[REDACTED]>; Mahoney, Maureen <[REDACTED]>  
<[REDACTED]>; Laird, Philip <[REDACTED]>  
**Cc:** Vanessa Gonzalez <[REDACTED]>; Julian Canete Pres/CEO <[REDACTED]>; Andrea Cao <[REDACTED]>; John Kabateck <[REDACTED]>; Lori Kammerer <[REDACTED]>; Hernandez, Marisa <[REDACTED]>; [REDACTED]; [REDACTED]; [REDACTED]  
**Subject:** Follow Up Letter from Oct. 21st Meeting

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello Ashkan and other CPPA staff members,

We wanted to send along this letter following our meeting a week ago, signed by the organizations that were in attendance, but representing the greater alliance consisting of more than 80 state and local business groups.

Please let us know if you have any questions or concerns.

Thank you,



**Nathan Haderlie**

Sr. Account Executive



[Website](#) | [Twitter](#) | [Facebook](#) | [Instagram](#)



CALIFORNIA  
HISPANIC  
CHAMBERS OF COMMERCE



November 1, 2022

Ashkan Soltani  
Executive Director  
California Privacy Policy Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

Dear Executive Director Soltani and Staff,

On behalf of California's leading small and ethnic businesses, industries, and job creators, we want to first thank you for your time and participation in our recent meeting to discuss our concerns and suggestions regarding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

We want to follow up our meeting with the tangible requests we discussed as an attempt to work together to make these policies work for both consumer privacy and allow businesses the ability to comply and adapt. Along with these recommendations, we want to address our concerns and confusion first.

- Small and medium-size businesses benefit from the internet. We can develop marketing programs and opportunities, reach potential customers, and operate our business at a much lower cost because of the information, data, and services that are available on the internet. If those products and services go away or become business costs, it will be much harder to compete with national and international businesses.
- The widespread confusion caused by the ever-changing rules leaves small and medium size businesses vulnerable to cybersecurity risks and scammers that are threatening them with liability lawsuits.
- A general opt-out signal (as defined in section 7025(c)(3) for receiving advertisements should not override business-specific settings made by the consumer. This rule as written could create confusion and unwanted notices for consumers.
- The Economic and Fiscal Impact Statement states its proposed regulations will have an initial compliance cost of \$128 for each of the 66,076 California businesses impacted by the newly created data privacy regulations. This is in stark contrast to the total initial cost of compliance of the California Consumer Privacy Act (CCPA) for businesses in California was estimated to be \$55 billion that was commissioned by the OAG and released in August 2019; this delta is alarming and suggests the CPPA's in-house analysis is incomplete.

- There could be long-term damage to California if regulators limit the use of anonymous data. The attached article from University of San Diego professor Orly Lobel questions the wisdom of prohibiting or discouraging the collections and use of data when that data plays an important role in crime prevention, public health, and other high priority issues impacting Californians.

Understandably, not every concern has a simple solution. We have a few things that the business community believes could be impactful but request the California Privacy Protection Agency consider.

- Postpone the enforcement date of July 1, 2023, to January 1, 2024, due to the delay in finalizing the CPRA regulations.
- Small businesses urge the agency avoid imposing indirect impacts on business owners, particularly as it relates to the impact on the cost and effectiveness of digital advertising.
  - Digital advertising costs
  - Social media advertising
  - Free/low-cost technical services (email servers, analytical tools, email marketing, etc.)
- Give businesses a 6–12-month compliance forgiveness window.
- Develop and execute upon a plan that will help business owners understand the complexities of the proposed regulations and requirements for compliance.

It is a critical time for consumers and small business owners -- Californians face high inflation, job reductions in the tech sector, and a potential recession. Now is the time to consider ways that allow businesses the ability to operate without adding more fees, regulations, and confusion. Thank you again for taking time to meet with members of our alliance.

Respectfully,

National Federation of Independent Business  
California Asian Chamber of Commerce  
California Hispanic Chambers of Commerce  
National Association of Women Business Owners  
Small Business California

---

**TIME**

## The Problem With Too Much Data Privacy

BY ORLY LOBEL

OCTOBER 27, 2022 6:30 AM EDT

Lobel is a Warren-Distinguished Professor and Director of the Center for Employment and Labor Policy (CELP) at University of San Diego. She is the author of *The Equality Machine: Harnessing Digital Technology for a Brighter, More Inclusive Future*

Privacy has long dominated our social and legal debates about technology. The Federal Trade Commission and other central regulators aim to strengthen protections against the collection of personal data. Data minimization is the default set in Europe by the GDPR and a new bill before U.S. Congress, The American Data Privacy and Protection Act, similarly seeks to further privacy's primacy.

Privacy is important when it protects people against harmful surveillance and public disclosure of personal information. But privacy is just one of our democratic society's many values, and prohibiting safe and equitable data collection can conflict with other equally valuable social goals. While we have always faced difficult choices between competing values—safety, health, access, freedom of expression and equality—advances in technology make it increasingly possible for data to be anonymized and secured to balance individual interests with the public good. Privileging privacy, instead of openly acknowledging the need to balance privacy with fuller and representative data collection, obscures the many ways in which data is a public good. Too much privacy—just like too little privacy—can undermine the ways we can use information for progressive change.

We rightfully fear surveillance when it is designed to use our personal information in harmful ways. Yet a default assumption that data collection is harmful is simply misguided. We should focus on regulating misuse rather than banning collection. Take for example perhaps the most controversial technologies that privacy advocates avidly seek to ban: facial recognition. 20 cities and counties around the U.S. have passed bans on government facial recognition. In 2019, California enacted a three-year moratorium on the use of facial recognition technology in police body cameras. The two central concerns about facial recognition technology are its deficiencies in recognizing the faces of minority groups—leading, for example, to false positive searches and arrests—and its increase in population surveillance more generally. But the contemporary proposals of unnuanced bans on the technology will stall improvements to its accuracy and hinder its safe integration, to the detriment of vulnerable populations.

These outright bans ignore that surveillance cameras can help protect victims of domestic violence against abuser trespassing, help women create safety networks when traveling on their own, and reduce instances of abuse of power by law enforcement. Facial recognition is increasingly aiding the fight against human trafficking and locating missing people—and particularly missing children—when the technology is paired with AI that creates maturation images to bridge the missing years. There are also many beneficial uses of facial recognition for the disability community, such as assisting people with impaired vision and supporting the diagnosis of rare genetic disorders. While class action and ACLU lawsuits and reform proposals stack up, we need balanced policies that allow facial recognition under safe conditions and restrictions.

We also need to recognize that privacy can conflict with better, more accurate, and less biased, automation. In the contemporary techlash, in which algorithms are condemned as presenting high risks of bias and exclusion, the tension between protecting personal data and the robustness of datasets must be acknowledged. For an algorithm to become more accurate and less biased, it needs data that is demographically reflective. Take health and medicine for example. Historically, clinical trials and health-data collection have privileged male and white patients. The irony of privacy regulation as a solution to exclusion and exploitation is that it fails to address the source of much bias: partial and skewed data collection. Advances in synthetic data technology, which allows systems to artificially generate the data that the algorithm needs to train on can help alleviate some of these tensions between data collection and data protection. Consider facial recognition again: we need more representative training data to ensure that the technology becomes equally accurate across identities. And yet, we need to be deliberate and realistic about the need for real data for public and private innovation.

An overemphasis on privacy can hamper advances in scientific research, medicine, and public health compliance. Big data collected and mined by artificial intelligence is allowing earlier and more accurate diagnosis, advanced imaging, increased access to and reduced costs of quality care, and discovery of new connections between data and disease to discover novel treatments and cures. Put simply, if we want to support medical advances, we need more data samples from diverse populations. AI advances in radiology have resulted not only in better imaging but also in reduced radiation doses and faster, safer, and more cost-effective care. The patients who stand to gain the most are those who have less access to human medical experts.

In its natural state—to paraphrase the tech activist slogan “Information wants to be free” (and channeling the title of my own book *Talent Wants to Be Free*)—data wants to be free. Unlike finite, tangible resources like water, fuel, land or fish, data doesn’t run out because it is used. At the same time, data’s advantage stems from its scale. We can find new proteins for drug development, teach speech-to-text bots to understand myriad accents and dialects, and teach algorithms to screen breast mammograms or lung x-rays when we can harness the robustness of big data—millions, sometimes billions, of data points. During the COVID-19 pandemic, governments track patterns of the spread of the disease and fight against those providing false information and selling products under fraudulent claims about cures and protections. The Human Genome Project is a dazzling, paradigmatic leap in our collective knowledge and health capabilities enabled by massive data collection. But there is much more health information that needs to be collected, and privileging privacy may be bad for your health.

In health care, this need for data is perhaps intuitive, but the same holds true if we want to understand—and tackle—the root causes of other societal ills: pay gaps, discriminatory hiring and promotion, and inequitable credit, lending, and bail decisions. In my research about gender and racial-pay gaps, I’ve shown that more widespread information about salaries is key. Similarly, freely sharing information online about our job experiences can improve workplaces, and there are initiatives concerning privacy that may inadvertently backfire and result in statistical discrimination against more vulnerable populations. For example, empirical studies suggest that ban-the-box privacy policies about criminal background checks for hiring may have led to increased racial discrimination in some cities.

Privacy—and its pervasive offshoot, the NDA—has also evolved to shield the powerful and rich against the public’s right to know. Even now, with regard to the right to abortion, the legal debates around reproductive justice reveal privacy’s weakness. A more positive discourse about equality, health, bodily integrity, economic rights, and self-determination would move us beyond the sticky question of what is and is not included in privacy. As I recently described in a lecture about *Dobbs v. Jackson Women’s Health Organization*, abortion rights are far more than privacy rights; they are health rights, economic rights, equality rights, dignity rights, and human rights. In most circumstances, data collection should not be prevented but safeguarded, shared, and employed to benefit all.

While staunch privacy advocates emphasize tools like informed consent and opt-out methods, these policies rely on a fallacy of individual consent. Privacy scholars agree that consent forms—those ubiquitous boilerplate clickwrap policies—are rarely read or negotiated. Research also reveals that most consumers are quite agnostic to privacy settings. The behavioral literature calls this the privacy paradox, revealing that in practice people are regularly willing to engage in a privacy calculus, giving up privacy for perceived benefits. So privileging privacy is both over and under-inclusive: It neglects a fuller array of values and goals we must balance, but it also fails to provide meaningful assurances for individuals and communities who have an undeniable history of being oppressed by the state and privileged elite. The dominance of privacy policy can distort nuanced debates about distributional justice and human rights, as

we continue to build our digital knowledge commons. Collection of important data to tackle our toughest social issues is a critical mandate of democracy.