March 12, 2019

Chairman Roger Wicker  
Ranking Member Maria Cantwell  
Members, Senate Committee on Commerce, Science, & Transportation  
512 Dirksen Senate Building  
Washington, DC 20515

Re: Policy Principles for a Federal Data Privacy Framework in the United States

Dear Chairman Wicker, Ranking Member Cantwell, and Members of the Committee:

The Software & Information Industry Association (SIIA) is pleased to provide this statement for the record on the February 27, 2019 hearing entitled “Policy Principles for a Federal Data Privacy Framework in the United States.”

SIIA is the principal trade association for the software and digital information industries worldwide. SIIA’s membership (nearly 800 companies and growing) includes the global industry leaders for the digital age, including software, data analytics, and information service companies. SIIA’s member companies reflect the broad and diverse landscape of digital content, including both B2B and B2C services, small specialized providers, and large multinational industry leaders. In some cases, these content services are completely free and ad-supported. In others, they are provided through a combination of subscriptions and ad-support.

SIIA endorses the passage of a comprehensive federal privacy law that will provide strong and meaningful consumer protections (such as individual rights to notice, access, control, correction, deletion, and portability), permit socially beneficial uses of consumer data, and promote innovation and competition in the American economy. To achieve these goals, a U.S. federal privacy law should be uniquely American in its inspiration, origin, and design; reflecting our constitutional safeguards, jurisprudential traditions, political sensibilities, and innovative marketplace.

SIIA urges Congress to consider three important objectives when creating a national framework. First, and paramount, new federal privacy legislation must ensure meaningful privacy protections for U.S. citizens. The legislation should both protect consumers from harm caused by the unreasonable collection and misuse of their personal data, and prevent and remedy data practices that injure consumers. While certain aspects of the European Union’s General Data Protection Regulation (GDPR) and the California Privacy Protection Act (CCPA), may be instructive, we urge the Committee to avoid their failings, particularly with respect to standards that could violate free speech principles as applied to public record information.

Second, a new federal privacy law must continue to promote a thriving internet and information-driven economy, where robust interstate and international information flows fuel the innovation that drives strong economic growth, employs millions of Americans, and
provides transformative benefits for consumers. To do this, Congress must harmonize the U.S. approach to privacy through one national standard.

Finally, privacy protections must be backstopped by meaningful enforcement, and Congress should make appropriate changes to the FTC’s authority to enable that enforcement. More specifically, Congress should give the FTC the resources it will need to enforce the law, as well as the ability to collect civil penalties for certain first-time violations. State attorneys general should also have an enforcement role.

The balance of our testimony describes each of these themes in more detail.

The Federal Privacy Law Must Prevent Harm and Provide Meaningful Consumer Protections

As noted above, the primary goal of new federal privacy legislation must be consumer protection that is designed to prevent harm resulting from the unreasonable collection or use of consumers’ personal information. To achieve this, privacy protections should be robust, meaningful, principles-based, and focused on outcomes and consumer expectations rather than complex consent procedures, prescriptive interface designs, or formalistic documentation requirements.

Federal Legislation Should Bar Unreasonable or Harmful Data Practices

SIIA supports a new privacy law that includes a provision articulating the principle that unreasonable or harmful practices relating to the collection, dissemination, or use of consumers’ personal data are unlawful. The law should identify the consumer injuries the it seeks to prevent and remedy, drawing on the four categories of informational injuries identified by the Federal Trade Commission in its recent staff comment to the NTIA: (1) financial injury, (2) physical injury, (3) reputational injury, and (4) unwanted intrusion.\(^1\)

The law may also identify data collection, dissemination, and use practices that are per se unreasonable or harmful. For instance, the law could bar the use of information to commit fraud or the use of data for unexpected practices that are neither disclosed nor apparent from the transaction at the time personal data is provided.

Establish Individual Rights for Personal Data

SIIA endorses a federal privacy law that establishes the following core individual rights: notice, control, access, correction, deletion, and portability. Like other industry groups, SIIA supports a risk-based, balanced and tailored framework that recognizes legitimate interests in privacy, freedom of expression, safety and fraud prevention, assistance to law enforcement,

data security, and preventing more data processing than is necessary. These standards are already widely accepted by industry associations.²

Striking an appropriate balance to ensure meaningful individual rights against these considerations is crucial, or the new federal privacy law will reap unintended and harmful consequences to competing individuals, routine business operations, and the exercise of justice. Moreover, any new federal privacy law should avoid focusing on the expansion of consent requirements to the detriment of meaningful consumer control. A blanket opt-in regime that fails to account for the sensitivity of the data and consumer harm undermines meaningful control. The GDPR illustrated this risk when its implementation resulted in numerous consent requests to consumers that arguably have the effect of lessening, rather than increasing, the seriousness with which people take online privacy.

The U.S. should learn from the EU’s mistakes by enabling meaningful consumer control through a context- and outcomes-based framework. This framework should take into account all levels of data collection and use. For instance, choice may be implied or unnecessary in the context of data use contemplated by the nature of the transaction (such as the use of data for fulfillment purposes), or to maintain a relationship with the customer (such as first-party advertising). In addition, choice is unnecessary with respect to data collection and use practices relating to publicly available information. Such information is unambiguously public and non-sensitive as a matter of law. This is in contrast to data practices involving sensitive personal data, which may merit a heightened choice model.

**A Federal Privacy Law Should Ensure the Free Flow of Information in the Public Domain**

SIIA strongly endorses a federal privacy law that bars the unreasonable or harmful collection or use of consumers’ *personal* and *non-public* data. Any federal law should exclude publicly available information or information about individuals acting in their business capacity as opposed to personal capacities.³ These narrow and appropriate exclusions preserve existing and fundamental freedoms as well as protecting business models that provide important and legitimate services and purposes, (such as employment background checks, law enforcement

---


³ SIIA also supports exclusions for de-identified, aggregated, or pseudonymized data to the extent it cannot be reasonably linked to a particular consumer.
investigations, “know your customer” standards, and industry analyst and ratings services). Moreover, it ensures that any new federal law passes constitutional muster.

Publicly available information plays a vital role in ensuring the freedom of our press, creating an informed citizenry, enabling rapid and inexpensive access to credit for consumer purchases and business expansion, promoting public safety (by tracking terrorists and criminals), locating missing persons, and tracking down parents for child support payments, among other important and legitimate uses. SIIA’s members invest billions to gather information from publicly available sources and aggregate it into useable digital files, which they maintain, update, and make available to the public and institutional customers. It is wasteful, and illogical, to expect news organizations, child safety centers, law enforcement, business intelligence services, and companies in all sectors of the economy to maintain and create their own public record databases. Instead, they rely on these information intermediaries for accurate, relevant, and up-to-date information. Any federal law unnecessarily impeding the use of publicly available information will be disruptive to public safety, public knowledge, and corporate due diligence and risk management functions.

For similar reasons, the federal law’s definition of personal data should include an exemption for people acting in their business capacity. People acting as officers, directors, shareholders or principals of business entities do not have a reasonable expectation of privacy for data relating to their conduct in roles open to public evaluation or critical to business risk management functions. Narrowing the definition of personal data to capture data relating to an individual operating in a business capacity risks giving bad actors a right to conceal disreputable or illegal business behavior from other commercial actors.

SIIA believes that allowing its members to engage in these valuable activities represents sound public policy. The free flow of public record information, however, is enabled not only by current law but also by constitutional command. As the Supreme Court has instructed, “[i]f the acts of disclosing and publishing information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct.”4 A federal privacy statute of the kind that the Committee is considering must balance the consumer’s legitimate interest in privacy against other important interests, such as those required by the First Amendment.

The CCPA’s drafting errors are instructive. There, the definition of personal information applies to any item of information that “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”5 The definition excludes “publicly available” information lawfully obtained from

---


government records, “if [sic] any conditions associated with such information,” and “if that data is [not] used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.”

For reasons contained in the memorandum attached to our testimony as Appendix A, that definition violates the First Amendment in at least three different ways, and places the entire CCPA in constitutional jeopardy. First, the CCPA’s distinction between publicly and non-publicly available information constitutes a content-based restriction that will receive strict scrutiny—the most demanding test in constitutional law. Second, the definition is both vague and overbroad: it requires a publisher of public record information to know why information was collected in the first instance before making use of it. Third, it discriminates among speakers—permitting nonprofit entities to engage in any activity with personal information while limiting that of some for-profit entities. Any one of these defects could result in judicial invalidation.

To summarize, where a statute seeks to directly regulate and proscribe the transmission of information that has been released into the public domain by the government itself, or otherwise not subject to a reasonable expectation of consumer privacy, heightened constitutional scrutiny is warranted and the legislation may well not pass it. As currently composed, the CCPA does not. On both policy and constitutional grounds, we urge the Committee not to follow in its footsteps.

**A Consistent National Framework is Critical to an Effective U.S. Privacy Framework**

Currently, U.S. companies operate in a patchwork of state and local privacy laws that are often inconsistent and incompatible, and impose unnecessary divergent compliance costs. This balkanized approach for privacy results in significant and unnecessary compliance costs to businesses that operate across state lines, unequal privacy standards for U.S. citizens, and consumer confusion as their privacy rights change as they travel and interact with businesses subject to diverse array of localized privacy regulations. Meanwhile, the U.S is losing ground as a global leader on privacy despite the fact that privacy has been a foundation of American common law since 1890 when Louis Brandeis and Samuel Warren published the “The Right to Privacy.” It is critical that the U.S. develop a national privacy standard that sets the pace for our modern dedication to privacy, protects American innovation and ingenuity, and re-emerges the United States as a global thought leader on this cardinal issue for the information age.

To achieve these important goals, preemption is imperative. It is the only way to ensure robust and meaningful protections, equal protection for Americans irrespective of their state of residence or location when engaging as customers, and to promote the free flow of data throughout the United States. Europe’s GDPR is instructive here. GDPR created a unified European approach to data protection, eliminating the risks associated with differing rules

---

6 *Id. 1798.140 (o)(2).*
across member states. Setting aside whether GDPR gets it right when it comes to meaningful consumer protection, what it certainly does is create a unified standard, predictability, and universal protections across the EU.

Equally important, a unified approach, like the GDPR, sets the standard for interstate and foreign commerce that depends upon cross-border data flows. The reality is that data collection and use involve a truly national information market that exists in interstate and foreign commerce. It is not an intrastate issue. This is evidenced by the U.S. support for mechanisms to facilitate cross-border data flows, including our accession to the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CPBR), our commitment to the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks, and the United States Mexico Canada Agreement’s recently negotiated chapter on digital trade that provides for a binding cross-border data flow obligation. A national framework for privacy supports and bolsters these efforts to preserve the ability to engage in cross-border data flows, which is integral to our information market.7

Data Security Regulations

SIIA recognizes that data security is integral to protecting the privacy of consumers’ personal data, and that the current security legal landscape (much like privacy) involves a number of overlapping, inconsistent, and confusing data security laws across states and localities. We support a new federal privacy law providing a harmonized data security standard to create equal protections for consumers and regulatory predictability for businesses. Much like the standard employed by the FTC in its data security program under Section 5 of the FTC Act, the new federal standard should require reasonable and appropriate security measures, the exact nature of which will depend on the sensitivity of the data, the risk of tangible harm from an unauthorized disclosure, the size and complexity of the business, and the availability and costs of the security features. The data security standard must be flexible, not overly prescriptive so as to risk staleness from the moment of enactment, and (like the privacy standard) focused on risk- and outcome-based standards.

A Federal Privacy Law Should Enshrine Principles of Strong Enforcement

SIIA supports a federal privacy law that continues and expands on the implementation, enforcement, and interpretation powers of the Federal Trade Commission (FTC). The FTC has long been the nation’s top privacy cop, beginning in the 1970s with its enforcement of the Fair

---

Credit Reporting Act. The agency has the expertise, knowledge, and skills to lead enforcement of a harmonized U.S. approach to privacy.

To ensure that the privacy law is comprehensive and technology- and industry-neutral, any new federal legislation should expand the FTC’s enforcement for purposes of privacy enforcement to cover common carriers and possibly non-profits, depending on whether the privacy law takes into account reasonable application standards for small businesses. Moreover, SIIA supports the allocation of increased budget resources to the FTC to ensure it has the staff, technologies, and other resources necessary to effectively deploy its enforcement mandate under the new law. With respect to remedies, the new law should provide the Commission with civil penalty authority for original violations, provided that the authority is appropriately calibrated to address risk-based personal data collection and use practices that cause tangible consumer harm. In other words, any grant of civil penalty authority for original violations should take into account whether the practice causes informational injury. Similarly, SIIA recognizes that a new federal law may merit the delegation of rulemaking authority to the Commission relating to some provisions in the legislative text, but we note that any textual grant of authority should include clear guidelines and require the tying of such regulations to the prevention of tangible consumer harms.

Although SIIA calls for primary enforcement authority to rest with the FTC, we recognize and endorse the important role for the States with respect to enforcement of a new federal privacy framework. To ensure a consistent application of the federal privacy law, the right of action to the States should include a concomitant obligation to notify the FTC prior to filing suit and grant the FTC a right of intervention.

**Conclusion**

SIIA appreciates the opportunity to provide the Committee with our comments to the recent hearing on “Policy Principles for a Federal Data Privacy Framework in the United States.” We are pleased to endorse the passage of a comprehensive federal privacy law that provides consumers with robust protections, follows our American common law and constitutional traditions, and promotes continued market innovation and growth. SIIA and our member companies look forward to working with the Subcommittee as the process moves forward. Please contact Sara DePaul, Senior Director of Technology Policy, at (202) 789-4471 or sdepaun@siia.net with any further questions or requests for further information.

Respectfully submitted,

Jeff Joseph, President
Software & Information Industry Association
Appendix A
MEMORANDUM

Date: January 24, 2019

To: Christopher Mohr
General Counsel
Software and Information Industry Association

From: Andrew J. Pincus
Miriam R. Nemetz
Eugene Volokh

Subject: Invalidity Under The First Amendment Of The Restrictions On Dissemination Of Accurate, Publicly Available Information Contained In The California Consumer Privacy Act of 2018

The California Consumer Privacy Act of 2018 (CCPA) violates settled First Amendment principles by restricting the dissemination of accurate, publicly available information. If the Act is not amended to eliminate these unconstitutional speech restrictions, it is highly likely to be invalidated in court.¹

Under the CCPA, California residents will be able to block businesses from selling “personal information” relating to them. The Act’s definition of “personal information” is not limited to private, sensitive data—it also encompasses information obtained from publicly available sources, such as information released to the public by government agencies. If the Act takes effect in its current form, individuals will be able to veto the inclusion of public-domain

---

¹ I write on behalf of the Software Information & Industry Association (SIIA) and the Coalition for Sensible Public Record Access (CSPRA). As you know, SIIA’s members include publishers of business-to-business and business-to-consumer products in both digital and print form, as well as financial news services, software companies, and databases. Through their independent news-gathering and publishing activities, SIIA’s members inform businesses, journalists, and governments on a wide variety of activities. CSPRA is a non-profit organization dedicated to promoting the principle of open public record access to ensure consumers and businesses the continued freedom to collect and use, for personal and commercial benefit, the information made available in the public record.

Some of the publications produced by the members of these groups include names and other information about individuals. Many other businesses—including industry analysts, marketing experts, executive search firms, agents, lobbyists, ratings services, private detectives, and many others—also gather and sell information about people. These publications are an important resource for users investigating potential employees, investors, business partners, clients, service providers, customers, and competitors.
information about them in the databases and publications that many businesses provide to customers who use them for important, entirely legitimate purposes. For example:

- businesses conduct background checks on potential employees and on the officers and directors of potential business partners and merger or acquisition candidates;
- law enforcement officers obtain information relevant to their investigations regarding persons of interest;
- financial institutions and other businesses employ third parties to use publicly available data sources to help them meet “know your customer,” anti-money laundering, anti-terrorism and anti-human trafficking obligations, as well as other financial crime and modern slavery laws, regulations, and industry practices; and
- industry analysts and ratings services obtain information critical to their analyses.

The Supreme Court has made clear that “the creation and dissemination of information is speech for First Amendment purposes.” *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011). The State may not infringe these rights to protect a generalized interest in consumer privacy. See generally E. Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049, 1081 (2000).

The CCPA’s extraordinarily broad definition of “personal information” and the resulting restrictions on businesses that sell publicly available information—restrictions unprecedented in American law—violate the First Amendment in at least three independent ways:

- **First,** the CCPA’s restrictions on the dissemination of publicly available information impose a heavy burden on protected speech without advancing a compelling governmental interest, or even a substantial one. These provisions therefore violate the First Amendment rights of the businesses whose speech is burdened by them, as well as of potential users of the information that the businesses provide.
- **Second,** the law suffers from the independent constitutional flaw that it adopts an unjustified and impermissibly vague standard for determining when a business may disseminate information from public government records.
- **Third,** the Act discriminates among speakers and discriminates on the basis of speech content, which separately violates the First Amendment.

To avoid the need for a judicial challenge to the provisions at issue, the Legislature should amend the Act to eliminate these unconstitutional speech restrictions.

I. **Background.**

The CCPA applies to “personal information,” which it defines broadly to encompass all information that “identifies, relates to, describes, is capable of being associated with, or could
reasonably be linked, directly or indirectly, with a particular consumer or household.” Cal. Civ. Code § 1798.140(o)(1).

“Personal information” excludes “publicly available information,” but the CCPA adopts an unusually narrow definition of the latter term. Cal. Civ. Code § 1798.140(o)(2). The definition first states that “publicly available” information means “information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information.” Id. It continues that “[i]nformation is not ‘publicly available’ if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.” Id.

The statute provides no guidance for determining when the sale of information obtained from public government records is “not compatible with” the purpose for which the data was maintained or made available by a governmental source. See Cal. Civ. Code § 1798.140(o)(2). Data “made available from federal, state, or local government records” therefore qualifies as personal information that is subject to the Act’s obligations and restrictions, depending on the meaning of the undefined “compatibility” test.

Importantly, the Act does not exclude from the definition of “personal information” any information that is available to the public but was not derived from governmental records. Thus, under the statute, a business may be precluded from selling information about a person that it gathers from phone directories, media outlets, and other widely available sources.

The CCPA—which takes effect on January 1, 2020—imposes obligations on any business that collects consumers’ personal information, does business in the State of California, operates for profit or for the benefit of its shareholders (thereby excluding non-profit entities), and either (1) has more than $25 million in annual revenue; (2) annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices; or (3) derives 50 percent or more of its annual revenues from selling consumers’ personal information. Cal. Civ. Code § 1798.140(c).

First, the Act requires businesses to disclose to consumers the types of personal information that it collects from them, to provide them with copies of the information, and to delete the information upon request. Cal. Civ. Code §§ 1798.100, 1798.105, 1798.110(a)-(b).

---

2 The sweeping definition includes, but is not limited to, a consumer’s “name, . . . physical characteristics or description, address, telephone number, . . . education, . . . [or] ‘employment history.’” Cal. Civ. Code § 1798.140(o)(1)(B) (incorporating Cal. Civ. Code § 1790.80). It also includes “[i]nferences drawn from any of the information identified . . . to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.” Id. § 1798.140(o)(1)(K).

3 This definition appears to be missing key words.

4 The Act defines “consumer” to mean any California resident who is natural person. Cal. Civ. Code § 1798.140(g).
Second, the Act also imposes obligations with respect to personal information that a business obtains from sources other than the consumer (which it defines broadly in Cal. Civ. Code § 1798.140(e) as a business that obtains such information “by any means”).

- The business must, upon request, disclose to the consumer the categories of personal information about that consumer that the business has collected, the purposes for which the information was collected, the categories of third parties with whom the business shares personal information, and the specific information that it has collected about that consumer. Cal. Civ. Code § 1798.110(a)-(b).

- If the business sells or discloses a consumer’s personal information for a business purpose, it must, upon request, provide the consumer with detailed information about such sales or disclosures. Cal. Civ. Code § 1798.115.

- Any consumer “shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information.” Cal. Civ. Code § 1798.120(a). Businesses must notify consumers that they have the right to “opt out” of the sale of their personal information. Id. § 1798.120(b).

II. The Act’s Restrictions On The Dissemination Of Accurate, Publicly Available Information Violate The First Amendment.

The CCPA’s provisions restricting the dissemination of publicly available information are unconstitutional for three independent reasons. First, these limitations are content-based restrictions on speech that are not justified by a sufficiently weighty governmental interest to satisfy strict scrutiny, or even intermediate scrutiny. Second, the regulation limiting dissemination of information publicly disclosed by government agencies is unconstitutionally vague. Third, the CCPA’s restrictions unconstitutionally distinguish among speakers and among different types of speech.

A. The Act’s limitations on speech are subject to strict scrutiny.

The First Amendment, which applies to the States through the Fourteenth Amendment, prohibits laws that abridge freedom of speech. Content-based regulations, which do not affect speech incidentally but instead “target speech based on its communicative content,” are “presumptively unconstitutional.” Reed v. Town of Gilbert, 135 S. Ct. 2218, 2226 (2015); see also, e.g., R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) (“Content-based regulations are presumptively invalid.”). “If a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest.” United States v. Playboy Entm’t Grp.,

---

5 The right to demand that businesses delete information about them is limited to information “which the business has collected from the consumer” (Cal. Civ. Code § 1798.105(a))—but the rights to demand that information be disclosed, and not be sold, lack such a limitation, and thus apply to information about people gathered from all sorts of sources.
Inc., 529 U.S. 803, 813 (2000). “If a less restrictive alternative would serve the Government’s purpose, the legislature must use that alternative.” Id.

The CCPA’s limits on dissemination of publicly available information plainly qualify as content-based regulations. The Act flatly prohibits certain businesses from selling the “personal information” of people who exercise their statutory right to opt out. Such a law does not affect speech incidentally but instead directly “imposes a burden based on the content of speech and the identity of the speaker.” Sorrell, 564 U.S. at 567. Indeed, under the Act, “the government is prohibiting a speaker from conveying information that the speaker already possesses.” Id. at 568 (internal quotation marks omitted). As “a content-based speech restriction,” the Act’s bar on the dissemination of personal information “can stand only if it satisfies strict scrutiny.” Playboy Entm’t Grp., Inc., 529 U.S. at 813.

The First Amendment standard applicable to the CCPA is not lessened because the law targets speech for which businesses receive compensation. The Supreme Court has emphasized that “the degree of First Amendment protection is not diminished merely because . . . speech is sold rather than given away.” City of Lakewood v. Plain Dealer Publ’g Co., 486 U.S. 750, 756 n.5 (1988). The Court has also observed that “a great deal of vital expression” “results from an economic motive.” Sorrell, 564 U.S. at 567; see also Smith v. California, 361 U.S. 147, 150 (1959) (“It is of course no matter that the dissemination [of speech by the claimant] takes place under commercial auspices.”); Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 501 (1952) (“That books, newspapers, and magazines are published and sold for profit does not prevent them from being a form of expression whose liberty is safeguarded by the First Amendment.”).

For that reason, laws that “establish[] a financial disincentive to create or publish works with a particular content” (Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd., 502 U.S. 105, 115 (1991)) are subject to strict scrutiny under the First Amendment. The Act meets that description: It imposes a powerful “financial disincentive to create or publish” certain works by prohibiting the sale of any publication containing the personal information of a person who has opted out.

The Supreme Court’s decisions do distinguish between “speech proposing a commercial transaction, which occurs in an area traditionally subject to government regulation, and other varieties of speech.” Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n of N.Y., 447 U.S. 557, 562 (1980); see also Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 66 (1983) (the “core notion of commercial speech” is “speech which does no more than propose a commercial transaction”) (internal quotation marks omitted). Laws that limit such speech are unconstitutional unless they “directly advance[]” a “substantial” governmental interest and are not “more extensive than is necessary to serve that interest.” Cent. Hudson Gas & Elec. Corp., 447 U.S. at 566.

But the regulations here reach a range of communications that do not propose any commercial transaction. For example, a business that publishes and sells information for use by other businesses is producing an information-based product, but that speech is not in the nature of advertising and does not qualify as “commercial speech.” As discussed above, moreover, the regulations will impede speech outside the commercial realm by speakers ranging from book
publishers to photographers. The Act’s limitations therefore must be assessed under the strict scrutiny test.

B. The Act’s limitations on the dissemination of publicly available information fail strict scrutiny, and fail even intermediate scrutiny.

The CCPA’s broad-brush restrictions on the dissemination of publicly available information are not narrowly tailored to further compelling governmental interests. Indeed, even if examined under the more permissive standard that governs commercial-speech regulation, the provisions are infirm because they do not “directly advance[]” a “substantial” governmental interest, and because they are more extensive than necessary to serve any such interest. Cent. Hudson Gas & Elec. Corp., 447 U.S. at 566. As in Sorrell, “the outcome is the same whether a special commercial speech inquiry or a stricter form of judicial scrutiny is applied.” 564 U.S. at 571.

The government cannot defend a speech restriction “by merely asserting a broad interest in privacy.” U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999). “[P]rivacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it.” Id.

Here, the privacy concerns animating the Act’s passage had a specific focus: They arose from businesses’ collection and dissemination of data gleaned from consumers’ online activities, shopping, and use of computerized devices, which left consumers vulnerable to security breaches and other risks. See California Senate Judiciary Committee Bill Analysis, A.B. 375, at 1-2 (June 25, 2018). The CCPA’s statement of purpose recites that “there is an increase in the amount of personal information shared by consumers with businesses”; that many businesses “collect personal information from California consumers” without their knowledge; and that “[t]he unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals,” including “financial fraud” and “identity theft.” Cal. Civ. Code § 1798.100.

Many of the Act’s provisions respond to these identified risks, but the Act also applies to a wide variety of businesses that gather and sell information about people who are not customers. Their communications do not present the risks that the Legislature identified—and the stated interests therefore do not justify the regulations imposed on such businesses.

The government’s interest in protecting consumers from businesses that track their activities, moreover, is not furthered by restricting the publication and distribution of publicly available information. The firms that publish such information do not exploit customer relationships to obtain it. Nor do they disseminate otherwise confidential information that will threaten an individual’s safety and security if released. Instead, they distribute data that is already in the public domain so that it can be used efficiently by businesses, news organizations, and others that need the information.

Much of this public information has been released by government agencies. In California, these agencies have both a statutory and a constitutional obligation to provide “access to
information concerning the conduct of the people’s business” (Cal. Const. art. 1, § 3(b)(1)), unless one of the statutory exceptions to disclosure applies. When a government agency “plac[es] the information in the public domain,” it “must be presumed to have concluded that the public interest was thereby being served.” Cox Broad. Corp. v. Cohn, 420 U.S. 469, 495 (1975). That is particularly true in California, because the Public Records Act exempts from disclosure records “the disclosure of which would constitute an unwarranted invasion of personal privacy” (Cal. Gov’t Code § 6254(c)); information available to the public therefore by definition falls outside that category. Businesses that facilitate access to such information serve the public interest underlying the California constitutional and statutory provisions—and the CCPA thus infringes on government interests rather than furthers them.

In adopting the Act, the Legislature also posited more generally that the right of privacy granted by the California Constitution confers “the ability of individuals to control the use, including the sale, of their personal information.” Cal. Civ. Code § 1798.100. But the constitutional right of privacy is not so broad. Although “[i]nformational privacy is the core value furthered by” the constitutional privacy right, the California Supreme Court has explained that “information is private” only when “well-established social norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity.” Hill v. Nat’l Collegiate Athletic Ass’n, 7 Cal. 4th 1, 35 (Cal. 1994); see also id. at 37 (“A ‘reasonable’ expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms.”).

In fact, there is no general expectation of privacy with respect to all personal information as defined by the Act. The right of access to information from public records is enshrined in the California Public Records Act and in the Constitution, which both “strike a careful balance between public access and personal privacy.” City of San Jose v. Superior Court, 389 P.3d 848, 852 (Cal. 2017). Most Californians know that a substantial amount of information about them can be obtained through a Google search and a review of public records, and there is no “indignity” in that state of affairs. Thus, the right of privacy does not trump a business’ First Amendment right to sell information in the public domain.

The Act’s restrictions also have the potential to reach a wide variety of communications. For example, the law could reach:

• political opposition research businesses that sell information about the people they are hired to investigate;

• freelance press photographers who sell “visual . . . information” about newsworthy people and events; and

• private detectives, who sell information about the people they are investigating.

Moreover, people will be able to demand that private detectives and opposition researchers—and even book publishers—disclose any information that they have gathered about them. Cal. Civ. Code § 1798.110(a)-(b). That would include information gathered in the course of investigations: People who learn that they are the subject of a forthcoming book or investigative
report can demand to promptly learn all the information that was confidentially gathered about them.

Nor do the statute’s narrow exceptions for free speech, journalism, and politics prevent such applications. The exception for a business’ right to “[e]xercise free speech” (Cal. Civ. Code § 1798.105(d)(4)) applies only to people’s right to delete information about them, under Section 1798.105; it does not apply to their right to demand that information about them not be sold, under Section 1798.120. Though journalism and politics are excepted from the definition of “commercial purposes” (id. § 1798.140(f)), publishing organizations with revenue of over $25 million or political research groups that earn more than 50 percent of their revenue from selling information about research subjects are still covered “business[es]” under Section 1798.140(c)(1); the statute’s prohibitions and requirements apply to them without regard to whether their purposes are viewed as “commercial.” And though Section 1798.145(k) provides an exception for the “noncommercial activities” of certain publishers covered by Cal. Const. art. I, § 2(b), those publishers are limited to broadcasters and publishers of periodicals, and do not include publishers of other works, such as books, databases of information, or nonperiodical research reports. See also Legislative Counsel’s Digest, S.B. 1121, § 2 (describing this exception as limited to “newspapers and periodicals”).

Even if the publication of particular types of governmental information could be appropriately limited on the ground that widespread dissemination would lead to “unjustified embarrassment” (Hill, 7 Cal. 4th at 35), that would not save the statute from invalidation. “In the First Amendment context, . . . a law may be invalidated as overbroad if a substantial number of its applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” United States v. Stevens, 559 U.S. 460, 473 (2010) (internal quotation marks omitted).

The CCPA is fatally overbroad, because it gives consumers the right to veto a large number of communications as to which they have no legitimate privacy right. The statute is thus facially invalid even if a small subset of its applications would be appropriate. See Stevens, 559 U.S. at 473. If a compelling governmental interest would be served by limiting the further dissemination of certain public information, then that interest can be advanced by a statute that narrowly targets the troubling information.6 But the Act’s extensive burdens on speech cannot be justified on the ground that a small fraction of the information should be protected.

The Act’s restrictions on dissemination of certain information are invalid for the additional reason that they are fatally underinclusive—the CCPA does not prohibit a number of indistinguishable means of disseminating widely the very same information. Information excluded from publications under the Act may still be distributed by businesses not covered by the Act, in newspaper and magazines (which are generally excluded from the Act), and in innumerable other ways, including on Facebook, Instagram, or Twitter.

No substantial governmental interest in consumer privacy is advanced by singling out certain businesses and prohibiting them from transmitting personal information when many other

individuals and businesses (including any nonprofit entities and smaller businesses) may continue to share the very same information. As the Supreme Court has held, the “facial under-inclusiveness” of an information privacy law “raises serious doubts” about whether it serves any genuine governmental interest at all. *Fla. Star v. B.J.F.*, 491 U.S. 524, 540 (1989) (striking down law barring publication of rape victims’ names by mass media where the provision did not “prohibit the spread” of the information “by other means,” such as “the backyard gossip who tells 50 people that don’t have to know”).

In sum, the asserted interests in privacy do not justify the broad and unfocused restrictions on dissemination of publicly available information that the Act imposes. These provisions thus violate the First Amendment.

C. The exception for publicly available information from governmental records is both impermissibly narrow and unconstitutionally vague.

The CCPA suffers from the independent, constitutional flaw that it adopts an unjustified and impermissibly vague standard for determining when a business may disseminate information from public government records.

As discussed above, the Act excludes from the definition of “personal information” “information that is lawfully made available from federal, state, or local government records,” unless “that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.” Cal. Civ. Code § 1798.140(o)(2). The compatibility requirement, which in other contexts restricts the sharing of personal information among governmental agencies, is not an appropriate standard for limiting the dissemination by private parties of information that an agency has publicly disclosed. The Act itself, moreover, articulates no standard for discerning whether use of a particular category of government information is “compatible” with the purpose for which the government maintained or released the information. Thus, even if the State could articulate a substantial interest in limiting the sale of information that a governmental agency has made public, the vagueness of this provision renders the Act’s restrictions invalid under the First Amendment.

The concept of compatible use appears to have been modeled on analogous language in the federal Privacy Act’s “routine use” exception. The Privacy Act governs federal agencies’ use and disclosure of information about individuals, such as information about an individual’s education, financial transactions, medical history, criminal record, and employment history. 5 U.S.C. § 552a(a)(4). Under the Privacy Act, an agency may not disclose such information to other individuals or agencies without the prior consent of the person to whom the record pertains, unless the disclosure is authorized by one of several statutory exceptions. Id. § 552a(b). Under one such exception, an agency may disclose information to another agency for a “routine use” (id.), which means “the use of such record for a purpose which is compatible with the purpose for which it was collected.” Id. § 552a(a)(7). A disclosure cannot be authorized under the routine use exception unless the disclosing agency first publishes a notice describing “each routine use of the records contained in the system, including the categories of users and the purpose of such use.” Id. § 552a(e)(4)(D).
The Privacy Act’s “compatible use” requirement is “intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency’s reasons for using and interpreting the material.” Brit v. Naval Investigative Serv., 886 F.2d 544, 555 (3d Cir. 1989) (quoting Analysis of House and Senate Compromise Amendments to the Federal Privacy Act, reprinted in 120 Cong. Rec. 40,405, 40,406 (1974)). Similar requirements have been incorporated in laws that govern information-sharing by some California agencies. See, e.g., Cal. Code Regs. tit. 15, § 2087(c)(1)(A) (allowing disclosure of personal information maintained by the Parole Board to a state agency if “the transfer is compatible with a purpose for which the information was collected”); id., tit. 5, § 42396.2(d) (“Personal information should not be transferred outside The California State University unless the transfer is compatible with the disclosed purpose for which it was collected”).

Because the “compatible use” requirement was designed to protect privacy by limiting the disclosure of confidential personal information, it is not an appropriate standard to govern the use of information after the agency has released it to the public. Cf. Fla. Star, 491 U.S. at 534 (making clear that, even when an agency has broad power not to release information about a person, once that information is released, the public is generally free to redistribute it). Under the Privacy Act, the determination whether a particular use is compatible requires “a dual inquiry into the purpose for the collection of the record in the specific case and the purpose of the disclosure.” Brit, 886 F.2d at 548-49. Some courts have required “a nexus approaching an identity of purpose . . . between the reason the information was collected and the proposed routine use.” U.S. Postal Serv. v. Nat’l Ass’n of Letter Carriers, AFL-CIO, 9 F.3d 138, 144 (D.C. Cir. 1993). Were that standard applied to the dissemination of publicly disclosed information by private parties, it would prohibit virtually every such use because agencies generally do not maintain or release their records for the purpose of having their records republished. It would also excessively burden speech by requiring a case-by-case determination of the agency’s purpose in maintaining the records and its compatibility with the proposed use.

Were a court to conclude instead that the Privacy Act precedent is inapplicable, then the provision would be unconstitutionally vague because the statute provides no guidance for determining whether a proposed use of governmental information is “not compatible” with the government’s purpose in maintaining or releasing it. A content-based regulation that is vague “raises special First Amendment concerns because of its obvious chilling effect on free speech.” Reno v. ACLU, 521 U.S. 844, 871-72 (1997). “[V]ague laws chill speech” because “[p]eople ‘of common intelligence must necessarily guess at [the law’s] meaning and differ as to its application.’” Citizens United v. FEC, 558 U.S. 310, 324, (2010) (quoting Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926)). “The prohibition against vague regulations of speech” also is motivated by concerns about the “risk of discriminatory enforcement.” Gentile v. State Bar of Nev., 501 U.S. 1030, 1051 (1991).

The Act’s “compatible use” requirement raises both concerns: It is so ambiguous and unclear that many businesses will forgo disseminating governmental information rather than risk violating the provision, and it is so indeterminate that the risk of discriminatory enforcement is high.
Under the Privacy Act, agencies must disclose the purposes for which they may transfer information to another agency under the “routine use” exception. But agencies do not typically explain the reasons for which they release information to the public. Nor could they, because an agency gives up control of the information when it makes it available to the public without conditions. Because agencies may not even consider how the information that they release may be used, there is no consistent, predictable and non-arbitrary way to determine whether a particular use of publicly available government information comports with the agency’s intent. This makes it likely that such determinations will be made in an ad hoc and standardless manner that will single out certain uses for unfavorable treatment.

A familiar example illustrates the problem. Records of home sales often are made public, and the information is used for many purposes. Neighbors may look up the information out of curiosity, appraisers working for lenders or insurers may employ the information in valuing other properties, and local businesses may use the information to direct their marketing efforts. Such information also may be published in the real estate sections of magazines and newspapers and on websites such as Zillow and Redfin. If a California resident objected under the Act to a particular use of the information—such as the inclusion of his or her name, address, and home price in a guide to movie stars’ homes—it is anyone’s guess whether that use would be deemed “not compatible” with the purpose for which the information was made publicly available. The publisher thus would face the choice between removing the requester’s name from the publication or risking an enforcement proceeding.

Each type of publication of each category of government information will present a similar dilemma. Given the uncertainty surrounding the concept of “compatible use,” many publishers will hesitate to include certain types of government information in their publications. The vagueness of the “compatible use” requirement thus will substantially limit protected speech.

D. The regulations disfavor certain speakers and messages.

Laws that “disfavor[] specific speakers” or “speech with a particular content” (Sorrell, 564 U.S. at 564) rarely survive First Amendment scrutiny. See Rosenberger v. Rector & Visitors of Univ. of Va., 515 U.S. 819, 828 (1995) (“In the realm of private speech or expression, government regulation may not favor one speaker over another.”).

The CCPA on its face favors some speakers and some uses of information while disfavoring others. It also allows consumers to use the power of the State to suppress particular speakers and facts. And it does so in a frankly content-based way, aiming at restricting the publication of certain information but not other information. See Reed, 135 S. Ct. at 2227 (concluding that content-based speaker restrictions are subject to strict scrutiny); Citizens United, 558 U.S. at 340 (same); Sarver v. Chartier, 813 F.3d 891, 903 (9th Cir. 2016) (holding that statute that restricts the commercial use of people’s personal identifying information “clearly restricts speech based upon its content”). The CCPA therefore violates the fundamental First Amendment principle against distinguishing among speakers in a number of different ways.

First, the Act selectively burdens the speech of a subset of businesses that maintain and sell personal information—those that have substantial revenues, those that receive or disseminate
the personal information of large numbers of users for commercial purposes, and those that derive more than half of their annual revenues from the sale of personal information. Cal. Civ. Code § 1798.140(c). The Act requires these businesses to provide consumers with an “opt-out” right and bars them from selling information about people who exercise the right, but imposes no such requirements on smaller businesses that generally distribute different sorts of information (aggregated in different ways) than the larger businesses do. Furthermore, the opt-out right is limited to information that is sold; consumers may not block the distribution of personal information for other business purposes unless the information was collected from the consumer. Id. §§ 1798.105(a), 1798.120(a). The Act thus disfavors large businesses and smaller businesses that depend on selling personal information.

Second, the Act discriminates among speakers in another way: It provides that “the rights afforded to consumers and the obligations imposed on any business” under the Act “shall not apply to the extent that they infringe on” the activities of persons engaged in journalism and connected with a “newspaper, magazine, or other periodical publication, or . . . a press association or wire service.” Cal. Civ. Code § 1798.145(k); Cal. Const. art. I, § 2(b).

Thus, the Los Angeles Times could not be stopped from sharing information about a California resident’s criminal record with millions of daily readers, but that person could bar other businesses—including, for instance, book publishers—from including the same information in their publications. Because “[t]he law on its face burdens disfavored speech by disfavored speakers” (Sorrell, 564 U.S. at 564), and does so based on content and not just speaker identity, it violates the First Amendment.

Third, the law’s practical effect is to enable California residents to suppress the communication of particular facts. By exercising their opt-out rights, consumers can prevent a business from disseminating information about them in any communication that the business sells. The veto right conferred by the statute is virtually absolute: As long as the information satisfies the definition of “personal information,” the consumer may direct the business not to sell it, and the business must comply. Indeed, unless the business decides to give away its products rather than sell them, the restriction imposed once an individual opts out amounts to a “complete speech ban[].” 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 501 (1996). Such bans, “unlike content-neutral restrictions on the time, place, or manner of expression, are particularly dangerous because they all but foreclose alternative means of disseminating certain information.” Id. (internal citation omitted).

Moreover, the Act authorizes consumers to ban speech selectively, allowing some businesses to speak about them while silencing others. “[A] law or policy permitting communication in a certain manner for some but not for others raises the specter of content and viewpoint censorship.” City of Lakewood, 486 U.S. at 763.

Indeed, the Act appears designed to encourage such censorship. A California resident may first review the personal information that a company maintains and then decide whether to employ his or her opt-out right. Thus, a consumer may permit continued sales of positive information but block sales by businesses that possess negative information. Individuals can also favor some speakers over others: They can direct one business not to sell personal information while allowing
another business to market the very same information. This creates the potential for groups of consumers to burden disproportionately the speech of unpopular speakers, effectively censoring their communications in a manner that violates First Amendment principles.

III. The Act Should Be Modified To Exclude All Publicly Available Information.

Businesses whose speech is burdened by the CCPA will able to sue in federal court under 42 U.S.C. § 1983 to assert their First Amendment rights and obtain an order invalidating the statute. Successful plaintiffs will be entitled to an award of attorney’s fees and costs under 42 U.S.C. § 1988. To avoid the need for expensive litigation, the Legislature should amend the Act to remedy the First Amendment violations identified here. This can be achieved, in part, by modifying the definition of “publicly available information” to include both information that is “lawfully made available to the general public from federal, state, or local government records,” without exception, and other information that is generally available to a wide range of persons, such as information from telephone books, information published in newspapers, and information from other public media.