ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

March 8, 2019

Mr. Xavier Becerra
Attorney General
Department of Justice
State of California
300 S. Spring St.
Los Angeles, CA 90013

RE: The California Consumer Privacy Act, Assembly Bill 375, Rulemaking Process

Dear Attorney General Becerra,

The Information Technology & Innovation Foundation (ITIF) is pleased to submit these comments in response to the California Justice Department's rulemaking process for the California Consumer Privacy Act (CCPA).[1] CCPA establishes new consumer data protection rights and creates new requirements for businesses collecting and handling personal information. ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington, and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation, and productivity.

At the outset, it is important to note that while ITIF supports the California Attorney General's efforts to bring regulatory certainty and clarity to California businesses and consumers regarding how the new rules will affect them, the State of California has significantly increased the regulatory costs and complexity on businesses by enacting a sweeping state-level data privacy law. Businesses operating online often find themselves subject to duplicative and conflicting laws because many countries claim jurisdiction over their activities.[2] Subnational governments, like states, should not compound the problem by adding their own layer

[1] "California Consumer Privacy Act (CCPA)," *Office of the Attorney General of California*, accessed February 19, 2019, https://oag.ca.gov/privacy/ccpa.
[2] Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy" (Information Technology and Innovation Foundation, September 2014), http://www2.itif.org/2014-crossborder-internet-policy.pdf.

of additional rules and regulations, especially in areas already regulated, like data protection. Doing so across all states is unsustainable because it would introduce unnecessary and unreasonable compliance costs on businesses, making it more difficult for businesses to scale nationally and thereby undermining U.S. competitiveness. Given the threat to the digital economy of multiple state laws and Congress's ongoing efforts to develop national data privacy legislation, the Attorney General's office should make clear that it supports a single federal law that preempts states.

The California Department of Justice is currently going through its preliminary rulemaking activities and anticipates publishing a Notice for Proposed Regulatory Action on CCPA this fall.[3] Moreover, the California Attorney General has recently endorsed legislative changes to the CCPA.[4] ITIF welcomes the opportunity to provide input on how the California Attorney General on both the current statute and proposed amendments to minimize compliance costs and damage to digital innovation while ensuring consumer protections.

While the California Department of Justice continues to pursue its obligations under the CCPA, there are several factors it should consider:

- Do not enforce CCPA outside of California
- Clarify exemptions for data protected by existing laws
- Reform, but do not remove, the 30-day cure
- Provide businesses with guidance on compliance
- Adjust transparency and access requirements
- Do not prohibit beneficial incentives to data sharing
- Do not expand the private right of action

BACKGROUND

California has a number of privacy laws already in statute, including those that require companies to disclose what data has been used for direct marketing, give notice to consumers in the event of a data breach, and

[3] "CCPA Public Forum," *Office of the California Attorney General*, accessed February 25, 2019, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-ppt.pdf.
[4] "Attorney General Becerra, Senator Jackson Introduce Legislation to Strengthen, Clarify California Consumer Privacy Act," *Attorney General Xavier Becerra*, press release, February 25, 2019, accessed March 6, 2019, https://oag.ca.gov/news/press-releases/attorney-general-becerra-senator-jackson-introduce-legislation-strengthen.

provide greater protections for health data than those offered by federal law. Adding to these laws, California passed the CCPA in June of 2018, which will go into effect on January 1, 2020.[5]

CCPA makes several changes to California privacy statute. It expands the definition of personal data from traditionally protected categories, such as health data and social security numbers, to include new types of information, such as location data, device identifying numbers, and biometric information.[6] It requires businesses to notify consumers of what personal data they are using and how they are using it.[7] It also provides users with the ability to opt out of having their personal information shared with a third party.[8] Californians can also request that businesses delete their personal data.[9] Businesses are prohibited from discriminating against consumers that exercise their rights under the act, such as by charging a different price or providing a different level or quality of goods or services, but they can offer consumers financial incentives to allow personal data collection.[10]

CCPA has several enforcement provisions. The act expands Californian consumers previous right of action by allowing them to sue for damages if their personal information "is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices."[11] Consumers are entitled to penalties of between $100 and $750 per incident in damages.[12] However, before consumers can bring a lawsuit, businesses have a 30 day grace period to address the violation and provide consumers with an express written statement saying the issue has been fixed and further violations will not occur.[13] Regarding government enforcement, CCPA gives the Attorney General broad authority to enforce the act, with fining authority of $2,500 per violation or $7,500 for each intentional violation.[14] However, here again businesses have a 30-day grace period to fix the problem.

---

[5] The attorney general is required to publish final regulations for the law before July 2020, which will go into effect six months later.
[6] California Consumer Privacy Act, California Civil Code, § 1798.140.
[7] California Civil Code, § 1798.115.
[8] California Civil Code, § 1798.120.
[9] California Civil Code, § 1798.105.
[10] California Civil Code, § 1798.125.
[11] California Civil Code, § 1798.150 (a).
[12] California Civil Code, § 1798.150 (a)(1)(A).
[13] California Civil Code, § 1798.150 (b).
[14] California Civil Code, § 1798.155 (b).

Businesses can also seek out the opinion of the Attorney General for guidance about how to comply with the CCPA.[15]

In recent weeks, the Attorney General has supported a bill to make changes to the CCPA. Introduced by California State Senator Hannah-Beth Jackson, SB 561 would significantly change these enforcement provisions.[16] First, the bill would expand individual's right of action to all violations under the act. Second, it would remove the 30-day cure for enforcement by the Attorney General. Finally, it would remove the ability of businesses to seek advice from the Attorney General regarding compliance with CCPA. These changes would negatively affect the welfare of both Californian businesses and residents.

The rulemaking process is set to help the California Department of Justice clarify several things with the CCPA, including: 1) categories of personal information, 2) definitions of unique identifiers, 3) exceptions to CCPA, 4) submitting and complying with requests, 5) uniform opt-out buttons, 6) notices and information to consumers, including financial incentive offerings, and 7) verification of consumer requests.[17]

DO NOT ENFORCE THE CCPA OUTSIDE OF CALIFORNIA'S JURISDICTION

CCPA applies to many businesses that handle personal data about Californians. The law applies to businesses operating in California if they generate an annual gross revenue of $25 million or more, if they annually receive or share personal information of 50,000 California residents or more, or if they derive at least 50 percent of their annual revenue by "selling the personal information" of California residents.[18] In effect, this means that businesses with websites that receive traffic from an average of 137 unique Californian IP addresses per day could be subject to the new rules. The CCPA does not apply to nonprofits or the small number of businesses that do not meet any of these thresholds.

If the Attorney General broadly interprets which entities this law applies to, it would create administrative costs for many businesses nationwide that have little to no relationship with the state. For example, a company operating out of Maine with a revenue of $26 million could be subject to these rules if it has a single Californian customer. Or an online media business based in Florida that averages 150,000 visitors per day

[15] California Civil Code, § 1798.155 (a).
[16] California Consumer Privacy Act of 2018: Consumer Remedies, S.B. 561, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200SB561.
[17] "CCPA Public Forum."
[18] California Civil Code, § 1798.140.

worldwide could be subject to this law if 150 of those visitors come from California. The result of this would be an incentive for some companies outside of California to stop selling to California residents, or block them from their website, just as the EU's General Data Protection Regulation led some U.S. companies to block Europeans from their sites.[19]

Moreover, if other states follow California's lead, many online businesses, large and small, would face multiple state laws. For example, Californian businesses might be subject to 49 additional state laws. Such an outcome would impose unreasonable compliance costs on businesses, subject them to conflicting laws from other states, and threaten the viability of a national market for digital services.

Instead, the Attorney General should use its discretion to apply this statute only to businesses with a significant presence in the state. This could mean businesses that have offices, employees, bank accounts, physical property, or substantial marketing in California, or those that engage in significant business activity within the state. Moreover, in its final rulemaking, the Attorney General should explicitly state the parameters in which it will subject out-of-state businesses that fall outside of these criteria to enforcement actions. By doing so, the state can clarify the requirements for businesses with nexus in California without impeding on other states' jurisdictions. If the Attorney General does not believe it has the discretion to limit its application of CCPA in this way, it should recommend that the state legislature amend the law.

CLARIFY EXEMPTIONS FOR DATA PROTECTED BY EXISTING LAWS

The CCPA exempts certain information already covered under certain federal laws, such as financial information covered by the Gramm-Leach-Bliley Act (GLBA), driving information covered by the Driver's Privacy Protection Act (DPPA) of 1994, credit information covered by the Fair Credit Reporting Act, health information covered by the Health Insurance Portability and Availability Act (HIPPA) of 1996, and certain types of personal information covered by California statute, such as the California Financial Information Privacy Act (CFIPA).[20]

Even with these exemptions, however, CCPA will create additional compliance costs for businesses already covered by rigorous privacy rules. For example, even though financial services companies are already subject

[19] Daniel Castro and Alan McQuinn, "GDPR Freeloaders: Why Other Countries Should Fight Back," *Information Technology and Innovation Foundation*, August 16, 2018, accessed March 7, 2019, https://itif.org/publications/2018/08/16/gdpr-freeloaders-why-other-countries-should-fight-back.
[20] California Civil Code § 1798.145.

to GLBA and CFIPA, the law does not exempt these companies from its obligations. This includes CCPA requirements to make disclosures to consumers for certain personal non-public financial information (i.e., data not covered by GLBA) and to provide certain rights to consumers, such as the consumers right to stop the business from sharing their personal information and the right to access.[21] The Attorney General should clarify these exemptions to industries with privacy regulations already in statute or harmonize state privacy regulations targeting sensitive types of information across industries. The overall goal should be to reduce the compliance burden on organizations, especially those already subject to federal or state data privacy regulations. If the Attorney General does not believe it has the authority to clarify these exemptions, it should call on the state legislature to amend the law.

REFORM, BUT DO NOT REMOVE, THE 30-DAY CURE

During enforcement of CCPA by the Attorney General, businesses are only in violation of the title if they fail to remedy an alleged violation within 30 days after being notified of alleged noncompliance.[22] However, the Attorney General, through its support of SB 561, is seeking to remove this provision, known as a "30-day cure," arguing that it would be able to secure more civil penalties and thus increase enforcement. Specifically, the Attorney General has said it needs to raise $57.5 million in civil penalties to cover the cost of CCPA enforcement.[23]

This is the wrong approach. The goal of data privacy legislation should not be to maximize fines on the private sector, but rather to increase consumer protections while minimizing costs to the economy and preserving innovation. The 30-day cure is a useful provision that should be preserved because it allows companies to focus on compliance by giving them an opportunity to address alleged harms. This means that companies can still innovate quickly as long as they are responsive to any potential violations. This flexibility is especially important in the digital economy—which California specializes in—where companies iterate quickly on products and services. New technologies, consumer offerings, and business models are continuing

[21] Timothy Tobin and Roshni Patel, "California Consumer Privacy Act: The Challenge Ahead – The Interplay Between CCPA and Financial Institutions," *Hogan Lovells*, December 7, 2018, accessed February 25, 2019, https://www.hldataprotection.com/2018/12/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-the-interplay-between-the-ccpa-and-financial-institutions/.
[22] California Civil Code, § 1798.155.
[23] Janine Anthony Bowen et al., "Overview of the new California Consumer Privacy Law," *BakerHostetler*, January 1, 2019, accessed March 6, 2019, https://www.dataprivacymonitor.com/wp-content/uploads/sites/5/2019/01/Overview-of-the-New-California-Consumer-Privacy-Law.pdf.

to emerge. In such an environment, consumer protection regulation needs to ensure that it is not so strict and punitive as to harm innovation, especially in cases where there was no intent to do harm and where no harm occurred. This provision would allow companies to work with the Attorney General to resolve any alleged problems and make consumers whole without exposing those companies to high legal fees.

The 30-day cure should not be a free pass for misbehavior. For example, if a company intentionally commits consumer harm, but fixes the problem within 30 days, they should still be subject to enforcement. Surely, the Attorney General would not want CCPA to inadvertently create a sanctuary for those committing material consumer harms. In addition, the CCPA does not specify how the Attorney General should enforce similar violations of the act that occur after the 30-day window. For example, imagine a vulnerability in a company's system leads to a data breach, and while the company takes action to fix the initial problem and makes customers whole, two months later there is a second data breach based on a different bug that causes consumer harm. Would the Attorney General treat these issues separately with 30-day compliance windows, or would the company be immediately subject to penalties for the second violation? The Attorney General's office should clarify its policies around enforcement of this provision.

Rather than seek to remove the 30-day component entirely, the Attorney General should seek an update to the CCPA that clarifies the 30-day cure. The CCPA should give the Attorney General discretionary authority to bring enforcement actions based on two factors: the extent to which a company acted intentionally or negligently, and the extent to which a company's action caused real, substantial consumer harm.[24] The act should still give businesses that did not act intentionally or negligently, or did not cause substantial consumer harm, a period of time to fix their compliance issues. Importantly, the Attorney General should not subject companies to punitive measures for actions they take in good faith that did not cause consumer harm because doing so would force companies to prioritize regulatory compliance rather than preventing consumer injury. This would create perverse incentives for Californian businesses, such as by pushing them to hire privacy lawyers to rewrite their online terms of service to minimize legal exposure from a data breach rather than hiring security experts to remedy cybersecurity vulnerabilities.[25]

[24] Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene" (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-how-whenregulators-intervene.pdf.
[25] Ibid.

PROVIDE BUSINESSES WITH GUIDANCE ON COMPLIANCE

The CCPA enables businesses to seek the opinion of the Attorney General for guidance on how to comply with its provisions.[26] However, the Attorney General supports SB 561 which would remove this provision.[27] The Attorney General argues it should not need to "provide, at taxpayers' expense, businesses and private parties with individual legal counsel on CCPA compliance."[28]

Again, the Attorney General has misplaced priorities. If the goal is to increase compliance with data privacy rules, the Attorney General should welcome the opportunity to clarify to industry what practices are acceptable or not acceptable. Providing this information would also allow the Attorney General to outline permissible conduct without resorting to expensive and time-consuming enforcement actions. To do otherwise would create a chilling effect on innovation, as California businesses would be unable to go to market with a clear sense of risk of non-compliance with CCPA of a new product or service.

This type of relief is not an unheard-of practice. For example, many different agencies—both federal and state—offer the ability to send letters to companies, called no-action letters, saying that agency will not bring enforcement actions against a particular product or service.[29] The goal of these alternatives to enforcement is to reduce regulatory risk for companies and signal to the market what type of behavior is acceptable. By letting companies come to the Attorney General when their products and services do not fit neatly into predetermined guidelines within the CCPA, it will enable the regulator to have a more flexible and nuanced approach to unconventional technologies and business models—ensuring Californians' privacy is protected while also enabling innovation to proceed apace. The Attorney General should not seek to remove this positive provision of CCPA.

ENSURE TRANSPARENCY AND ACCESS REQUIREMENTS ARE NOT BURDENSOME

The CCPA gives users rights to transparency—ensuring organizations disclose how their information is used, the purposes for which it is used, with whom is it shared, users' rights under the law, and more—and a right

---

[26] California Civil Code, § 1798.155 (a).
[27] S.B. 561.
[28] "Attorney General Becerra, Senator Jackson Introduce Legislation to Strengthen, Clarify California Consumer Privacy Act," *Attorney General Xavier Becerra.*
[29] For example, see the Securities and Exchange Commission's (SEC) policy on No-Action Letters. "No Action Letters," *U.S. Securities and Exchange Commission*, March 23, 2017, accessed March 6, 2019, https://www.sec.gov/fast-answers/answersnoactionhtm.html.

to access their information.[30] It mandates that businesses promptly take steps to disclose and deliver, free of charge, consumers' personal information.[31] The right of transparency and access have clear benefits for consumers because it allows users with strong privacy preferences to make more informed choices. These provisions also will enable the California Justice Department to hold companies accountable for their promises.

However, the cost of providing data access could be substantial for many organizations, especially for large, old, and complex data sets, and data sets that are not digitized (e.g., stored on paper in filing cabinets).[32] Therefore, the Attorney General should use a reasonableness standard to interpret this statute. This right should be limited to require data controllers disclose whether they have data about a specific individual, the type of information collected, the policies governing that data collection, and with what other entities the organization has shared the data. This right should not apply to proprietary data, which is data about an individual that is inferred or computed by an organization. For example, companies construct online advertising profiles for consumers based on many different sources of observed personal information, such as direct-mail responses, search history, and demographic information. Finally, the right should only apply to sensitive categories of data. For example, patients should continue to be able to get access to their medical records at no cost, and consumers should have access to their utility usage data. Requiring access to nonsensitive data, such as publicly available personal information, device identifiers, and stored IP addresses, will only raise compliance costs with limited usefulness to the consumer. If the Attorney General does not believe it has the authority to limit these access requirements, it should recommend that the state legislature amend the law.

The Attorney General should also work to align the costs of this regulation with its benefits. Currently, the CCPA does not allow businesses to recoup any costs for providing consumers with any information required under the statute.[33] The Attorney General should call on the California legislature to allow companies to charge search, review, and duplication costs for providing data access—similar to what the federal government can charge individuals for requests made under the Freedom of Information Act.

---

[30] California Civil Code, § 1798.100.
[31] Ibid.
[32] Alan McQuinn and Daniel Castro, "A Grand Bargain on Data privacy Legislation for America" (Information Technology and Innovation Foundation, January 2019), 38-39, http://www2.itif.org/2019-grand-bargain-privacy.pdf.
[33] California Civil Code, § 1798.130 (2).

Moreover, many organizations do not have a process to easily verify someone's identity.[34] Poor verification of requests for personal information poses a substantial privacy risk to consumers. Therefore, the Attorney General should specify the permitted processed by which organizations can verify the identity of individuals requesting a copy of their data.

DO NOT PROHIBIT BENEFICIAL INCENTIVES TO DATA SHARING

CCPA prohibits businesses from denying goods and services or offering a different level of quality of service when users exercise their rights under the law.[35] The law does allow certain covered entities to offer different prices, rates, levels, or quality of goods and services to users if that difference is directly related to the value of the user's data. Covered entities can only offer this incentive program if they receive affirmative consent from the user prior to their participation in the program and allow them to opt out at any time. Moreover, CCPA forbids using this practice in an unjust, unreasonable, coercive, or usurious way.

Unfortunately, laws like the CCPA that restrict businesses from offering discounts to customers who share their data, including for targeted advertising, hurt both users and companies.[36] Companies benefit from these relationships by monetizing data through advertising (usually in ways that do not divulge personally identifiable information to advertisers) and realizing lower customer acquisition costs.[37] Consumers get direct benefits through lower prices as well as better and more customized offerings. Society also benefits from greater levels of efficiency in advertising with less money spent on poorly targeted ads.

Moreover, by restricting companies from limiting services or increasing prices for consumers who opt-out of sharing personal data, CCPA enables free riders—individuals that opt out but still expect the same services and price—and undercuts access to free content and services. Someone must pay for free services, and if individuals opt out of their end of the bargain—by allowing companies to use their data—they make others pay more, either directly or indirectly with lower quality services. CCPA tries to compensate for the drastic

[34] See the following article written by a Californian florist. Jim Relles, "Another Voice: The New California Privacy Law Will Hurt Sacramento Small Businesses," *Sacramento Business Journal*, February 28, 2019, accessed March 7, 2019, https://www.bizjournals.com/sacramento/news/2019/02/28/another-voice-the-new-california-privacy-law-will.amp.html.
[35] California Civil Code, § 1798.125.
[36] McQuinn and Castro, "A Grand Bargain on Data privacy Legislation for America," 26-30.
[37] Alan McQuinn, "No, Internet Users Are Not Paying With Their Data," *Inside Sources*, August 7, 2018, accessed March 7 ,2019, https://www.insidesources.com/no-internet-users-not-paying-data/.

reduction in the effectiveness of online advertising, an important source of income for digital media companies, by forcing businesses to offer services even though they cannot effectively generate revenue from users. Online advertising is most effective when advertisers can serve relevant ads. Targeted ads based on information about a user (e.g., browsing history) help deliver higher-value ads. If regulations reduce the effectiveness of targeted ads, websites—especially those offering free services—will get less revenue.[38] In effect, by enabling users to access online services without providing the information necessary for companies to monetize those services, the CCPA could create a free-rider problem for online services.

Reducing the effectiveness of advertising may result in some companies, particularly those with thin margins, switching to a fee-for-service or subscription business model, wherein customers would have to pay for services that used to be free.[39] While this change would mean slightly lower living standards for everyone who switches, many low- and middle-income Californians would simply lose access to beneficial services they would not wish to pay for or could no longer afford. Moreover, because a subscription-based model would result in reduced revenues, it would also likely decrease the quality, breadth, and variety of content.

To mitigate against the risk created by prohibiting businesses from penalizing users that do not consent to data sharing, the Attorney General should interpret this statute to only apply to companies charging discriminate prices or those that offer a substantially different product or service to users that choose to opt-out. The Attorney General should not consider companies blocking users from accessing services to be a violation of this provision or from charging them a reasonable market price. Moreover, the Attorney General should clarify publicly that businesses are allowed to take either of these actions. Companies should not be forced to give free services to individuals that exercise their right to not contribute their data and thus deprive companies of the revenue necessary to operate those services. They should also be permitted to charge consumers a fair market price for any of their services.

---

[38] Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use" (Information Technology and Innovation Foundation, July 11), https://itif.org/publications/2018/07/11/why-stronger-privacy-regulations-do-not-spur-increased-internet-use.

[39] Alan McQuinn, "The Detractors are Wrong, Online Ads Add Value," Information Technology and Innovation Foundation, December 8, 2016, accessed February 20, 2019, https://itif.org/publications/2016/12/08/detractors-are-wrong-online-ads-add-value.

DO NOT SEEK TO EXPAND THE PRIVATE RIGHT OF ACTION

The CCPA expands the private right of action in California by giving afflicted parties cause to sue for statutory damages in some cases where their data has been subject to unauthorized access or theft.[40] The Attorney General has endorsed SB 562, which would expand the private right of action to any violation under the act.[41]

Unfortunately, expanding the private right of action to violations of the CCPA that did not cause any consumer harm would make Californians worse off. Innovation by its very nature involves risks and mistakes. If CCPA exposes companies to massive liability every time they make those mistakes—no matter how small or if there is no consumer harm—there may be fewer mistakes, but there will also be significantly less innovation.[42] This change would actually make Californian consumers worse off overall as money is needlessly diverted to minimizing legal risk rather than lowering prices, offering discounts, or creating new products and services. Legal risk makes companies stop innovating around personal data. For example, grocery stores could stop offering coupons based on purchase history—hurting low-income consumers that use those discounts for frequency bought goods.

This scenario has occurred in Illinois, where a vaguely written law allows consumers to sue companies for using facial recognition technology without their permission, even in cases where there is no proof of actual damages.[43] As a result, Illinois has seen a significant rise in largely groundless, class-action lawsuits against tech companies, such as Facebook, Shutterfly, and Snapchat.[44] Because of the legal risk created by this law, Illinoisans do not have access to many fun and productivity-increasing products that use biometrics

[40] California Civil Code, § 1798.150 (a).
[41] "Attorney General Becerra, Senator Jackson Introduce Legislation to Strengthen, Clarify California Consumer Privacy Act," *Attorney General Xavier Becerra.*
[42] McQuinn and Castro, "A Grand Bargain on Data privacy Legislation for America," 61-62.
[43] Megan Brown, "Illinois: Actual Injury Not Required for Privacy Lawsuit; Inviting Costly Litigation against Innovators," *Wiley Connect*, January 25, 2019, accessed March 6, 2019, https://www.wileyconnect.com/home/2019/1/25/illinois-actual-injury-not-required-for-privacy-lawsuit-inviting-costly-litigation-against-innovators.
[44] Ally Marotti, "Shutterfly lawsuit tags Illinois as battleground in facial recognition fight," *Chicago Tribune*, September 21, 2017, accessed March 6, 2019, https://www.chicagotribune.com/business/ct-biz-biometrics-shutterfly-lawsuit-20170920-story.html.

technology.[45] The Attorney General should learn from the mistakes of Illinois and not seek to expand the private right of action to cases where there was no tangible consumer harm.

CONCLUSION

In implementing these rules, the California Attorney General's office should clarify its rules around jurisdiction, CCPA exceptions, and enforcement. It should also interpret these rules to minimize compliance burdens through the transparency and access provisions, as well as allow companies to create disincentives for free riders. To the extent it does not believe it has the authority to use its discretion in these ways, the Attorney General should seek legislative changes to that effect. Moreover, as the Attorney General seeks to amend CCPA, it should not support SB 561, which would reduce the California Department of Justice's flexibility in enforcement and increase compliance costs and legal risk for businesses throughout California.

To reiterate, ITIF believes the regulation of privacy rules affecting national entities should be left to federal authorities working in partnership with stakeholders from states, civil society, and the private sector. Rather than acting alone, California should work with federal policymakers to help create a meaningful U.S. privacy framework that balances consumer protections with support for data-driven innovation.

Sincerely,

Daniel Castro
Vice President, The Information Technology and Innovation Foundation

Alan McQuinn
Senior Policy Analyst, The Information Technology and Innovation Foundation

[45] Daniel Castro and Michael McLaughlin, "Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence" (Information Technology and Innovation Foundation, February 4, 2019), https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence.