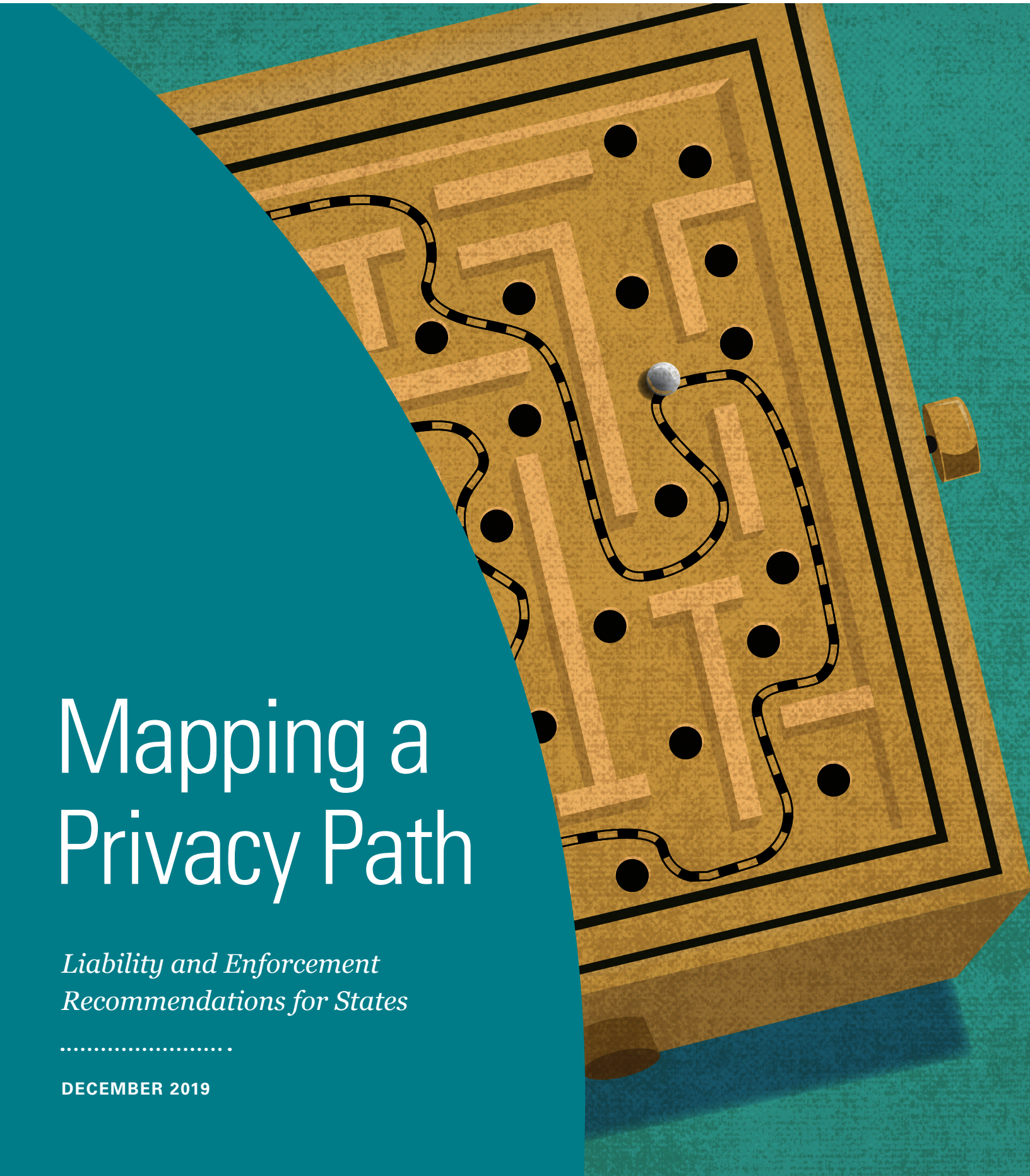
U.S. CHAMBER
Institute for Legal Reform



Mapping a Privacy Path

Liability and Enforcement Recommendations for States

DECEMBER 2019

U.S. CHAMBER
Institute for Legal Reform

An Affiliate of the U.S. Chamber of Commerce

Table of Contents

Prepared for the U.S. Chamber Institute for Legal Reform by

Megan Brown and Kat Scott, Wiley Rein LLP

Executive Summary

For consumers to reap the benefits of data-driven innovation, it is important that they can trust that their personal information is being protected. There is clearly a need for a unified national data privacy framework; but, to date, the U.S. Congress has not yet acted.

Meanwhile, states are not waiting on the federal government. State legislators across the country are considering and adopting laws. "Consumer data privacy legislation was introduced or considered in more than half the states in 2019, a substantial increase compared to previous years."[1]

A piecemeal approach is not ideal. It creates a confusing patchwork of laws and it increases compliance costs. Worse, it expands the risk of litigation and class actions that will enrich lawyers without benefitting consumers.

What Should State Policymakers Do?

The best approach to comprehensive privacy legislation is a unified federal privacy regime. But in the meantime, recognizing that states may be constrained to act, there are a number of interim solutions for state policymakers. These solutions are not focused on the substantive policy questions at the heart of the privacy and security debates. Instead, these solutions offer commonsense, procedural protections that will help to stem the tide of the state laws that risk "opening the door for opportunistic plaintiffs' lawyers to seek large settlements, even when there is no apparent harm."[2]

Each recommendation serves an important function to limit unintended consequences of state privacy and security laws by preventing unnecessary litigation.

THE POLICY RECOMMENDATIONS

Recommendation 1: Preclude Private Rights of Action	State privacy and security legislation should not include private rights of action—which provide no consumer protection benefits, impose heavy costs on legitimate businesses, and deter innovation.
Recommendation 2: Include Notice and Cure Periods	State privacy and security laws should ensure that covered organizations receive notice of alleged violations, as well as a reasonable opportunity to "cure" alleged violations, before they are subject to an enforcement action or litigation.
Recommendation 3: Offer Safe Harbors	State privacy and security legislation should include reasonable safe harbors for compliance.
Recommendation 4: Include Damage and Civil Penalty Caps	State privacy and security legislation should cap any damages or civil penalties for violations.
Recommendation 5: Define Enforcement Actors	State privacy and security legislation should specify that the state attorney general is the exclusive enforcer of state law.
Recommendation 6: Limit Attorneys' Fees	If state privacy or security laws allow private enforcement, they should limit attorneys' fees.
Recommendation 7: Curtail Municipality Litigation	State privacy and security legislation should prohibit enforcement by municipalities.

Recommendation 1: Preclude Private Rights of Action

State privacy and security legislation should not include private rights of action—which provide no consumer protection benefits, impose heavy costs on legitimate businesses, and deter innovation.

What Is the Issue?

Private rights of action provide consumers with the ability to sue organizations for violating a law. In the privacy and security context, private rights of action should be disfavored.

Some argue that private rights of action empower consumers to seek legal remedies for themselves, but this argument is misplaced. Privacy and security laws deal with complex and technical topics. Experts with discretion should lead consistent enforcement, and enforcement responsibility should not be placed with consumers or plaintiffs' lawyers. Granting enforcement of privacy laws to a public entity (ideally the state attorney general) will ultimately leave consumers better off.

> *"Private rights of action do not enhance consumer privacy; rather, they cater to the motives of plaintiffs' lawyers."*

Why Does This Matter?

FIRST

Private rights of action do not enhance consumer privacy; rather, they cater to the motives of plaintiffs' lawyers. Unlike the government—whose goal is, in part, to stop bad actors—the goal of plaintiffs' lawyers is to achieve the biggest payouts, which they accomplish by going after legitimate companies with deep pockets. These companies—regardless of whether they have done anything wrong—may be inclined or forced to settle instead of incurring litigation expense, the risk of costly damages, and bad press.

Plaintiffs' lawyers' infamous use of the Telephone Consumer Protection Act (TCPA) provides a great example of this: a comprehensive study of litigation brought

under the TCPA's private right of action found that "it is not the unscrupulous scam telemarketers that are targeted by TCPA litigation, but rather legitimate domestic businesses" that have resources to pay "lucrative settlements or verdicts."[3]

SECOND

Private rights of action impose costs on businesses that are: (1) not proportionate to the harms that the laws are trying to prevent; and (2) not targeted at true bad actors. Experience confirms this. The Illinois Biometric Information Privacy Act (BIPA) provides a private right of action for statutory violations, including violations of procedural provisions that do not result in any harm.[4] Seizing on the low hurdle to state a claim, plaintiffs have brought hundreds of BIPA suits in the past two years.[5] And because the statute provides for liquidated damages of $1,000 to $5,000 per violation, legitimate companies who have not engaged in any substantive privacy abuses face billions in liability.[6] Other statutes with private rights of action—like the TCPA or the Fair Credit Reporting Act—yield similar results.[7]

THIRD

Private rights of action place the enforcement burden on consumers rather than government actors who are equipped with expertise and discretion, and who are often more accountable. Many state privacy and security laws turn on ambiguous terms that make compliance difficult. Because these obligations are vague and fact-specific, state attorneys general (AGs)—not individual consumers—are best suited to bring cases alleging violations. AGs have discretion to bring, litigate, and settle appropriate cases, and they are subject to public accountability, unlike private plaintiffs' attorneys who may be motivated solely by large payouts and have no reason to take a reasonable interpretive approach to balance economic issues against an extreme view of the law.

"Private rights of action place the enforcement burden on consumers rather than government actors who are equipped with expertise and discretion, and who are often more accountable."

FOURTH

Private rights of action create an *in terrorem* effect that deters innovation. Companies may hesitate to roll out new and innovative products and services if there is a possibility that a consumer will bring a company-ending suit—even if the suit is ultimately meritless. This kind of hesitation or market aversion results in significant lost potential that is harmful to a dynamic, technology-based economy. After all, the information sector accounts for well over a trillion dollars in GDP[8] and nearly three million jobs in the United States.[9] Needlessly hampering industry will kill jobs and create deadweight loss.

What Is the Solution?

Fortunately, this problem has a straightforward solution: preclude private

rights of action in privacy legislation. Expert government actors—specifically AGs—should enforce privacy and security laws at the state level.

How Will This Help Consumers and the Economic Climate?

Excluding private rights of action strikes the right balance in protecting consumers and facilitating innovation and growth. Ultimately, it leaves consumers and industry better off.

- Vesting enforcement of privacy laws with a public entity (ideally the AG) will better serve the public interest. In contrast to the practice of plaintiffs' lawyers—coercing legitimate businesses with no real privacy issues to settle suits over ambiguous statutes—the government's incentive is to go after the practices that truly threaten consumer privacy.[10]

- Without the threat of massive damages for often minor missteps in legal gray areas, businesses will operate in a more stable economic environment, while striving to protect consumer privacy to avoid enforcement actions because it is good business.[11] Businesses should not have to fear that a good faith interpretation of a complicated statute will trigger a class action that could force them to close their doors.

> *"Excluding private rights of action strikes the right balance in protecting consumers and facilitating innovation and growth."*

State Legislation

State privacy and security legislation should: (1) prohibit private rights of action; and (2) vest exclusive enforcement authority in the state attorney general.

A diverse array of federal privacy legislation excludes private rights of action, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Children's Online Privacy Protection Act (COPPA), the Federal Educational Rights and Privacy Act, and the Genetic Information Nondiscrimination Act. HIPAA enforcement and oversight is "structured, thorough, and expansive enough to correct violations while including prescribed limitations so as not to cripple the industry with penalties and uncertainty." Similarly, COPPA has led to broad and effective enforcement, which protects consumer privacy without the bludgeon of class action litigation. And at the state level, Nevada's online privacy law, recently updated by SB 220, specifically states that "[t]he provisions ... do not establish a private right of action against an operator."[12]

State legislators should reject proposals to create private rights of action in privacy and security legislation and should state that new laws do not create the right to sue. Ultimately, states should leave privacy enforcement to law enforcers, not plaintiffs' lawyers.

Recommendation 2: Include Notice and Cure Periods

State privacy and security laws should ensure that covered organizations receive notice of alleged violations, as well as a reasonable opportunity to "cure" alleged violations, before they are subject to enforcement action or litigation.

What Is the Issue?

Privacy and security laws and regulations rarely keep pace with changing technology. Stagnant laws can leave organizations unsure about how to comply and how the law will treat their evolving practices. These laws are also highly complex, meaning that even companies with the best intentions may err when attempting to apply the laws in the real world. Companies deserve notice and a chance to course correct before being sued or subject to enforcement actions. The U.S. Supreme Court has invalidated laws that "fail[] to provide a person of ordinary intelligence fair notice of what is prohibited," because fair notice is a "fundamental principle in our legal system."[13]

Some privacy absolutists—and plaintiffs' attorneys—argue that cure periods constitute free passes to violate the law, but this is a red herring. Companies take formal notice of claimed violations seriously. Fining companies for not meeting a plaintiff's view of what was an adequate risk assessment or consent encourages novel claims. Questions about the legitimacy of a business's use of data are not black and white, and businesses want to comply with the law. Cure periods remove the "gotcha" approach.

> *"Companies deserve notice and a chance to course correct before being sued or subject to enforcement actions."*

> *It is contrary to everyone's interest—the government, businesses, and consumers—to punish willingly compliant parties for good faith missteps that can be resolved without litigation.*

Why Does This Matter?

Compliance is challenging for companies that are entering a new market where innovation is the norm, or where consumer demand for products and services is rapidly shifting. What is "reasonable" or lawful at one time may become obsolete as technology or consumer expectations change.

At the same time, privacy and security laws can impose complex requirements on covered organizations. For example, the California Consumer Privacy Act (CCPA) creates a number of consumer rights that are triggered in various contexts (depending on what type of information the organization has collected, what the organization is doing with that information, and who the consumer is) and that impose specific requirements. Navigating this type of law is very tricky, and even well-intentioned organizations could make a misstep.

Subjecting businesses operating in good faith to immediate enforcement actions or litigation for a decision or policy that is in a gray area or that is a technical mistake is bad policy.

Organizations want to comply with legal obligations. But they may need time to adjust practices to new regulations and, even after implementation, may face uncertainty about their legal obligations. They welcome guidance and an opportunity to take corrective action when a consumer or regulator considers a practice unlawful. It is contrary to everyone's interest—the government, businesses, and consumers—to punish willingly compliant parties for good faith missteps that can be resolved without litigation.

What Is the Solution?

A "cure period" solves these problems. A cure period—a well-developed principle derived from contract law—provides regulated parties an opportunity to fix a problem before incurring liability. Many statutes have adopted this principle for compliance with complicated laws.

How Will This Help Consumers and the Economic Climate?

Notice and cure periods help protect consumers in multiple ways.

- They encourage greater transparency and broader compliance, furthering the consumer protection goals of any privacy or security legislation. Notice and cure periods can help to change industry's response to complaints from a defensive, litigation-oriented mindset to a consumer-oriented mindset. By incentivizing businesses to resolve consumer complaints quickly and

without litigation, legislatures can ensure more widespread compliance with their substantive requirements.

- They free up valuable enforcement resources. If good faith businesses are actively adjusting privacy practices in response to notice, state enforcers will be able to focus resources on legitimately bad actors.

- They contribute to a flexible, collaborative privacy environment that is good for consumers and business. Privacy expectations change over time and across different settings. Giving businesses notice and an opportunity to change their practices allows companies to adjust to shifting consumer expectations, without subjecting them to unnecessary punitive measures.

- They create a more predictable business climate. A cure period allows good faith actors to come into compliance more quickly without the expense and delay of protracted litigation or government enforcement actions.

State Legislation

The touchstone for any notice and cure period provision should be clarity in process and a bar on litigation or enforcement: (1) during the notice and cure period; and (2) where good faith cure efforts are made.

Examples of cure periods exist and can serve as models for state policymaking.

- The Federal Trade Commission (FTC) Act provides a cure period in the context of warranty claims. "No action ... may be brought under subsection (d) for failure to comply with any obligation under any written or implied warranty or service contract, and a class of consumers may not proceed in a class action under such subsection with respect to such a failure ..., unless the person obligated under the warranty or service contract is afforded a reasonable opportunity to cure such failure to comply."[14]

- Civil rights laws often contain cure periods. For example, for certain claims under the Minnesota Human Rights Act, the law: (1) requires a would-be plaintiff to provide notice to an establishment with an alleged accessibility barrier; and (2) precludes any suit for 30 days to give the establishment time to cure the alleged violation.[15]

- The CCPA tempers its enforcement mechanisms with notice and cure periods. For the private right of action, the law requires consumers to provide written notice identifying the specific CCPA provisions the consumer alleges were violated; "[i]n the event a cure is possible, if within the 30 days the business actually cures the noticed

> *"A cure period—a well-developed principle derived from contract law—provides regulated parties an opportunity to fix a problem before incurring liability."*

violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur," the consumer cannot bring suit against the business.[16] For attorney general enforcement, a business only violates the law if it "fails to cure any alleged violation within 30 days after being notified of alleged noncompliance."[17]

Note that the CCPA's cure periods are not perfect because they appear to require de facto cures within a prescribed time. While this is better than no cure period, the recommended approach is to give businesses the opportunity to engage in good faith efforts to cure, as a complete fix may take longer than a statutorily enumerated time period.

- The U.S. Chamber of Commerce's Model Data Privacy Federal Legislation presents a path forward. It provides that "[b]efore proceeding with an enforcement action as authorized by this Section, the [Federal Trade] Commission shall notify a business that it has a reason to believe that the business has failed to comply with the Federal Consumer Privacy Act in a manner that is not willful or reckless. The Commission shall give a business reasonable time to cure non-willful or non-reckless violations before undertaking an enforcement action authorized by this Section."[18]

Notice and cure periods focus attention on fixing problems and protecting consumers, while reducing the opportunity to bring frivolous suits and play games. Any privacy law adopted by a state should have such a provision. State policymakers should draft and enact appropriate notice and cure provisions in any new privacy and data security law.

Recommendation 3: Offer Safe Harbors

State privacy and security legislation should include reasonable safe harbors for compliance.

What Is the Issue?

Businesses want to comply with their legal obligations and try to avoid uncertainty. Compliance with state privacy and security legislation can be difficult, given that these complex laws regulate a dynamic, high-growth field. One way that legislators can help these laws achieve their goals of protecting consumers—despite their complexities—is a safe harbor. Reasonable safe harbors will serve to encourage privacy and security best practices and processes and to protect well-intentioned companies from unfair, gotcha-style liability.

A "safe harbor" is defined as "[a] provision (as in a statute or regulation) that affords protection from liability or penalty."[19] While safe harbors can take many forms, an example would be a provision holding that an entity will not be liable for a violation of the given law if it meets certain conditions, such as having certain processes and procedures in place to ensure compliance. This type of provision encourages best practices and protects companies from liability for inadvertent missteps that can occur despite best efforts.

Why Does This Matter?

Businesses need guidance. Experts have explained that "[d]ata privacy laws and regulations are growing every day, and businesses are finding it increasingly difficult to comply and keep up with these fast-changing requirements."[20] "In the data protection and privacy context, businesses are frequently left having to speculate about what types of acts would be in violation of new regulations."[21]

In this environment, clear, practical, and tangible guidance can help businesses meet their growing compliance burden.

> *"[S]afe harbors give businesses certainty that the processes they are putting in place—which often require significant organizational resources—will actually meet or exceed the requirements of the law and protect them from liability."*

Safe harbors are proven regulatory tools to provide such guidance.

Additionally, safe harbors give businesses certainty that the processes they are putting in place—which often require significant organizational resources—will actually meet or exceed the requirements of the law and protect them from liability. This type of assurance goes a long way in incentivizing desired behaviors. In its absence—and in light of the complex and ever-developing state of privacy and security law—businesses lack certainty that their compliance efforts will protect them from liability. As a result, businesses may not invest as heavily in compliance programs until after the development of case law or enforcement patterns, to ensure they are adequately shielded from both.

What Is the Solution?

Reasonable safe harbors provide tangible guidance for businesses that want to achieve or exceed compliance. Safe harbors specify means for organizations to comply with a law and be shielded from liability. They are not the only way to comply, rather they provide one option for businesses to meet their statutory obligations. Safe harbors provide both tangible means and incentives to achieve desired behaviors.

> *"Compliance with safe harbors should preclude liability from both enforcement actions and private lawsuits."*

Some argue that safe harbors offer "free passes" to companies to avoid compliance and enforcement. But safe harbors do just the opposite, by incentivizing the exact behavior that the law requires in the first instance. If companies do not meet the conditions of the safe harbor, they can still be liable; if companies do meet the conditions of the safe harbor, then everybody wins. Safe harbors are simply another tool in legislators' toolboxes to ensure that companies are taking the right steps to protect consumer data.

How Will This Help Consumers and the Economic Climate?

Reasonable safe harbors provide organizations with a clear path to compliance. Because businesses will have guidance on how to fulfill their statutory obligations, they will be more likely to do so from the outset. This leads to improved outcomes for both consumers and the economic climate.

- Consumers will reap the benefits of better compliance in the form of greater privacy and data security protections.
- Businesses will be able to avoid costly enforcement actions and litigation, and better direct their resources to targeted compliance efforts. This will benefit consumers as well as businesses.
- Enforcers will be able to better allocate scarce government resources. Legitimate businesses will jump at the opportunity to achieve compliance

through a safe harbor, allowing enforcers to go after willfully or recklessly noncompliant organizations.

State Legislation

Compliance with safe harbors should preclude liability from both enforcement actions and private lawsuits. Without such assurances, safe harbor provisions will offer far less certainty and protection.

Safe harbors should also be reasonable. Imposing needlessly difficult-to-attain conditions will negate the benefits of safe harbors because businesses will not be able to meet such obligations. This is doubly true for small businesses—only 12 percent of the smallest businesses are highly confident in their knowledge of data protection and privacy regulations.[22] And small businesses—which have fewer resources to comply with privacy and data security laws—make up 99.9 percent of all American businesses.[23]

Safe harbors should incorporate process-based and existing, flexible standards, not prescriptive, technical conditions. Because privacy and data security are rapidly changing fields, regulators should avoid highly technical safe harbors. Instead, state legislation should offer safe harbors based on preexisting, flexible, and global standards. Relying on such standards accomplishes two goals at once: (1) it will provide certainty through process-based requirements while, at the same time, avoiding prescriptive technical conditions that will quickly become obsolete; and (2) it will help to harmonize compliance obligations for businesses, allowing for greater compliance with already-familiar regimes.

“Safe harbors should incorporate process-based and existing, flexible standards, not prescriptive, technical conditions.”

Several safe harbors exist in privacy and data security regimes that reflect these principles.

- The COPPA safe harbor program incorporates industry self-regulatory guidelines. Congress determined that to satisfy the COPPA requirements, operators can “follow[] a set of self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, approved [by the Federal Trade Commission].”[24] The FTC—an active and aggressive enforcer of COPPA—has approved multiple self-regulatory standards.[25]

- Ohio’s recently-enacted cybersecurity law provides a safe harbor for organizations that comply with well-known federal or international standards. Ohio’s law provides an affirmative defense for organizations that “[c]reate, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized

cybersecurity framework," including standards established by NIST—a federal, non-regulatory agency with deep expertise on cybersecurity—and international standards bodies, among others.[26]

- The U.S. Chamber's Model Data Privacy Federal Legislation provides a path forward. It mirrors COPPA's safe harbor framework, empowering the FTC to incorporate safe harbors through notice-and-comment rulemaking and requiring it to act on requests for safe harbor treatment within 180 days.[27]

Safe harbors benefit all stakeholders: businesses are better equipped to comply with state privacy and data security obligations, consumers receive enhanced protections as a result of more widespread compliance, and enforcers can focus resources on truly noncompliant organizations and bad actors. Any state privacy or data security law should include a safe harbor provision that is reasonable, precludes liability, and incorporates flexible preexisting standards.

Recommendation 4: Include Damage and Civil Penalty Caps

State privacy and security legislation should cap any damages or civil penalties for violations.

What Is the Issue?

Company-ending damages and enormous civil penalties are not needed to ensure that businesses comply with privacy and data security laws. The risk of tough but reasonable enforcement actions and lost consumer trust encourages businesses to protect consumer data. When mistakes are made, there should be accountability for bad actors. Privacy and security incidents are already extremely costly: "In the United States, the average cost of a data breach [was] $8.19 million in 2019 which is the highest cost globally ... [L]ost business was the largest of four major cost categories that contributed to the total cost of a data breach."[28] But state legislatures should not usher in an era of jackpot justice in privacy enforcement and litigation. They should place reasonable caps on any damages and civil penalties.

Why Does This Matter?

FIRST

Astronomical damages are not necessary to deter violations of state privacy and data security laws. Statutory damages are used as a deterrent for future violations, and businesses already have enormous incentives to protect consumer privacy. Recent survey data shows that more than half of consumers find that businesses' data privacy practices are "extremely important in influencing whether they'll do business with a company."[29] To put that in perspective, fewer consumers indicated that the "quality of the company's products and services" was as important.[30] Accordingly, businesses have strong market incentives to protect consumers' privacy.

The fallout from privacy and security incidents affects businesses' bottom lines in share value, lost goodwill, and out-of-pocket costs.[31] These very real costs can and do act as a deterrent.

Multi-billion-dollar fines and judgments make headlines and fill the coffers of government and lawyers. But they do little to advance security and privacy. Indeed, a recent and unprecedented $5 billion FTC fine against a major tech company was characterized as being less important than changes to governance and accountability structures.[32]

SECOND

Unlimited statutory damages have a terrible economic track record. For example, the TCPA provides for unlimited statutory damages of $500-$1500 per violation of the statute. As a result, the TCPA spawns thousands of lawsuits every year.[33] A TCPA plaintiff lawyer explains how to exploit statutory damages: "[Y]ou can collect between $500-$1,500 per unwanted call or text. That's right—up to $1,500 for each unwanted call or text. What you are going to see is that this can really add up fast. We have seen some folks get 100 calls or texts. I call it the joy of math."[34] About a third of TCPA suits are "putative class actions seeking statutory damages ranging from tens of millions to billions of dollars."[35] These kinds of unchecked damages can easily put companies out of business.[36]

THIRD

Uncapped statutory damages in privacy and security laws can chill innovation and stall the information economy. Because of the risk of staggering liability, uncapped statutory damages in state privacy and security legislation may discourage companies from making socially desirable investments to innovate in the dynamic and rapidly-growing information economy. After all, why would a company design an innovative new product or service if it carried the risk of bankrupting the company? The net result of this deterrence may be slower economic growth and missed opportunities.

What Is the Solution?

State privacy and data security legislation should include caps on civil penalties and/or damages. Caps allow for monetary fines but cut off liability at some dollar amount to prevent fatal damage to businesses in most cases.

Some argue that uncapped statutory damages are good because they scare businesses into compliance. But in reality, businesses already have a powerful incentive for staying on the right side of privacy laws—protecting consumer data

> *"Unlimited statutory damages have a terrible economic track record. [...] Because of the risk of staggering liability, uncapped statutory damages in state privacy and security legislation may discourage companies from making socially desirable investments to innovate ..."*

engenders trust. To the extent further deterrence from non-compliance is necessary, proportionate and fair penalties or damages can be built into statutes and enforced by state AGs, rather than by private plaintiffs' lawyers who are much more interested in making money than in ensuring compliance. Businesses need not be subject to company-ending damages to encourage compliance.

How Will This Help Consumers and the Economic Climate?

Capping penalties and damages allows for legislators to deter covered organizations from violating the law without also deterring innovation. Caps allow for legislators to draw a reasonable line to prevent exorbitant and disproportionate penalties that put companies out of business and slow down the dynamic and growing information economy.

Consumers will reap the benefits of innovation and more rapid job growth. Without fear that a single misstep might plunge them into bankruptcy, companies will be more willing to create dynamic new products and services to fuel the information economy. This certainty would have a major impact on the information sector of the U.S. economy, which already accounts for more than $1 trillion in GDP.[37]

With these caps, consumers will still receive the substantive protections of state privacy and security legislation. Because businesses will still fear enforcement actions—both because of monetary penalties and the potential for lost business—organizations will continue to have strong incentives to comply with state law.

Additionally, businesses will be subject to a significantly more stable economic environment. While organizations will still strive for compliance, they need not fear that any misstep in complying with a complex statutory regime will end their business.

State Legislation

Caps on civil liability should preclude liability beyond a reasonable amount, such that most businesses will not face economic ruin when trying to comply with a law in good faith. These caps are common throughout the United States in a number of different contexts.

- HIPAA—perhaps the most well-known federal privacy law—incorporates penalty caps. The caps are tiered based on the culpability of the violator (e.g., negligence versus "willful neglect").[38] For example, the low tier limits the penalty amount to "$100 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $25,000."[39]

- Many states cap damages for tort claims—especially where there is no economic harm, which is often the case in privacy violations.[40] For example, with

limited exceptions, Alabama provides that "in all civil actions where an entitlement to punitive damages shall have been established under applicable laws, no award of punitive damages shall exceed three times the compensatory damages of the party claiming punitive damages or five hundred thousand dollars ($500,000), whichever is greater."[41]

Reasonable caps on civil liability ensure that businesses are incentivized to comply with the law but do not face economic ruin for missteps. This better reflects the optimal balance between deterring violations and not discouraging innovation. Accordingly, any state privacy or data security law should include reasonable caps on civil penalties and/or damages.

"Reasonable caps on civil liability ensure that businesses are incentivized to comply with the law but do not face economic ruin for missteps. This better reflects the optimal balance between deterring violations and not discouraging innovation."

Recommendation 5: Define Enforcement Actors

State privacy and security legislation should specify that the state attorney general is the exclusive enforcer of state law.

What Is the Issue?

State AGs are best-positioned to enforce new state privacy and security laws. Spreading out enforcement authority beyond state AGs—to private plaintiffs, their attorneys, municipal governments, or other state agencies—risks inconsistent and unfair application of the laws by entities that lack expertise, accountability for statewide priorities, and the ability to coordinate investigations across the country.

State AGs play a central role in law and policy. An AG is typically authorized, by statute or the state constitution, to represent the state's interest in litigation affecting the state and its public policy. Although common law powers are defined differently in various states, they generally include the authority to "institute, conduct, and maintain all suits and proceedings ... necessary for the enforcement of the laws of the state."[42]

The key functions of a state attorney general are "control of litigation concerning the state; acting as the chief legal officer of the state; providing formal opinions to clarify the law; public advocacy; criminal law enforcement, primarily on the appellate level; law reform and legislative advocacy; and investigative authority."[43]

Why Does This Matter?

Privacy and security laws require policymakers to decide which entity should have enforcement power. Candidates include:

- State attorneys general
- Other state agencies
- Local government attorneys
- Private parties and their lawyers

Allowing private parties, multiple agencies, or municipalities to enforce privacy and security law further complicates an already complex patchwork of state privacy and security laws. Some would-be enforcers may be unfamiliar with complex consumer protection issues and unable to strike the right balance between enforcement and promoting innovation, which a state AG can do.

STATE AGS ARE MORE EFFECTIVE THAN PRIVATE PLAINTIFFS

Consumers and plaintiffs' lawyers do not have an incentive to promote consistent approaches that advance public policy objectives.

Consumers and plaintiffs' lawyers do not have the expertise, discretion, or accountability of the state AG.

Private rights of action enrich plaintiffs' lawyers without improving consumer privacy.

Private rights of action impose disproportionate costs on businesses perceived to have "deep pockets" instead of going after the true bad actors.

Private rights of action create an *in terrorem* effect that deters innovation.

STATE AGS ARE GENERALLY SUPERIOR TO OTHER PUBLIC ENFORCERS

State AGs have experience enforcing consumer protection laws, unlike municipalities or other government agencies.

Municipal enforcement can lead to a patchwork of interpretations and competing policy priorities within a state, complicating compliance efforts.

As the principal law enforcement officer of most states, state AGs are in the best position to harmonize the objectives of disparate statutes.

State AGs can work most effectively with other states and federal enforcement and policy authorities to investigate, litigate, and resolve coordinated actions.

Diffuse enforcement power can lead to over-enforcement, conflicting priorities, and divergent legal standards. It creates an unpredictable regulatory environment within a state and may undermine the policy of the state legislature. It also may interfere with the state AG's ability to collaborate effectively with peer AGs in other states and with the federal government in bringing and resolving matters.

What Is the Solution?

State privacy and security laws should give exclusive enforcement authority to state AGs, who can leverage their consumer protection expertise to exercise appropriate discretion and balance different—and often conflicting—public policy priorities.

Rulemaking and interpretive authority can give AGs flexibility to update the law as the privacy and data security ecosystems change. Such flexibility may prove to be important in the dynamic information economy. However, such authority should be limited. AGs should not be given a blank check to rewrite privacy rules each year, upsetting industry's confident reliance on current law and driving up compliance costs.

Legislators may consider giving state AGs advisory opinion authority, to help avoid costly enforcement actions and provide companies with consistent guidance to prevent violations of privacy and security laws.

How Will This Help Consumers and the Economic Climate?

FIRST

Consumers will benefit from an experienced enforcer that understands consumer protection issues and can promote consistent statewide policy.

State AGs have long been trusted to enforce consumer protection laws in complex environments.[44] Accordingly, they are best poised to weigh tradeoffs between deterring violations and not stifling socially and economically desirable behavior and innovation. Consumers will benefit when a state AG uses his or her discretion to promote an optimal mix of enforcement outcomes through a cohesive statewide strategy that effectuates the intent of the state legislature.

A state AG can coordinate enforcement priorities to target particularly harmful activity and advise the public on their rights. A statewide office is best positioned to provide a single point of contact for complaint resolution and for consumer tips and resources, as many already do.[45] Many states have broad consumer protection divisions that support education and other consumer protection activities.[46]

SECOND

The economic climate will benefit from exclusive enforcement by AGs because it will generate a more predictable regulatory environment. Unlike an enforcement regime that utilizes private parties, localities, or even other state agencies—each of which may have different interpretations and priorities—an AG can generate more uniform, harmonized enforcement policy. With this predictability, organizations will be better able to allocate resources and plan for the future.

> *"Diffuse enforcement power can lead to over-enforcement, conflicting priorities, and divergent legal standards."*

State Legislation

State legislators should vest exclusive enforcement authority with their AG.

- Washington and Texas each have biometric privacy laws enforced by their respective state AG. In Washington, for example, the law states: "This chapter may be enforced solely by the attorney general under the consumer protection act ... "[47]
- Nevada's recently-updated online privacy law vests enforcement authority solely with the state attorney general and specifies that the law does not establish a private right of action.[48]

State legislatures should ensure that their AG is the sole enforcer of any privacy or security law. Unlike plaintiffs' attorneys, municipalities, or a mix of other state enforcers, state AGs can create a cohesive statewide enforcement regime, which benefits consumers and businesses alike.

Recommendation 6: Limit Attorneys' Fees

If state privacy or security laws allow private enforcement, they should limit attorneys' fees.

What Is the Issue?

States should not provide private rights of action in privacy or security statutes; however, if they choose to go down this path, they should limit attorneys' fees. One of the main reasons private rights of action are ineffective is because plaintiffs' attorneys do not have incentives to vindicate the public interest but, instead, have incentives to seek massive payouts. This is particularly so in the context of class actions. As the U.S. Chamber Institute for Legal Reform has earlier observed, many class actions "are as a practical matter originated by plaintiffs' lawyers who then seek plaintiffs with standing to pursue the claims."[49]

The potential for astronomical attorneys' fees encourages litigiousness. For example, the Illinois BIPA and its uncapped statutory damages leads to astronomical potential attorneys' fees. Given that the expected payout for plaintiffs' attorneys has no limit, it is unsurprising that BIPA litigation and class actions in particular have exploded. Hundreds of suits are filed each year.[50]

Likewise, class actions have been brought over vulnerabilities in connected consumer products in the Internet of Things (IoT), even where there is no exploitation, breach, or harm. Because there is a potentially large class and substantial attorneys' fees, plaintiffs' firms have seized on these types of cases and publicize their settlements.[51] As one attorney in a class action said, "you'll end up with a snowball effect that takes off quickly. The plaintiffs' bar is talking about this. They're salivating over this. It's going to be a feeding frenzy."[52]

"Given that the expected payout for plaintiffs' attorneys has no limit, it is unsurprising that BIPA litigation and class actions in particular have exploded. Hundreds of suits are filed each year."

> *"'The plaintiffs' bar is talking about this. They're salivating over this. It's going to be a feeding frenzy.'"*

Privacy and breach litigation can lead to enormous settlements which often benefit attorneys more than consumers. Plaintiffs' attorneys often collect millions of dollars, while consumers may obtain only pennies or coupons. Some settlements award nothing to consumers at all, instead giving money—called "cy pres" awards—to groups with little connection to the litigation or entities that sue companies.[53] However, lawyers always get their cut.

Why Does This Matter?

The availability of large attorneys' fees can distort incentives to bring and conclude cases. This problem is particularly acute in the privacy context, where some courts do not require a showing that a plaintiff was injured. In these circumstances, plaintiffs' lawyers are able to secure enormous damages that are not really about making a consumer or client whole.

FIRST

Excessive attorneys' fees incentivize substantially more litigation than is socially optimal. If plaintiffs' lawyers are able to win attorneys' fees far in excess of the harms they are attempting to rectify, then by definition, enforcement resources are being inefficiently allocated. This is exactly what is happening.

In a recent high-profile breach settlement, "only $31 million of the settlement is available for ... cash payments" to the victims, whereas the victims' lawyers "will receive $77.5 million in fees, plus an additional reimbursement of up to $3 million in litigation expenses."[54]

SECOND

Over-enforcement by plaintiffs' attorneys hurts businesses and deters beneficial innovation, with no corresponding benefit to consumers. Plaintiffs' attorneys do not have an incentive to go after the really bad actors. Rather, they go after the companies with the deepest pockets. As the U.S. Chamber Institute for Legal Reform has long observed, "too many cases are filed based on the ease with which a settlement may be extracted—with little or no focus on whether there is serious consumer harm. And too many cases are settled with illusory benefits to class members and large fees for lawyers."[55]

This helps explain why a multi-billion-dollar BIPA suit is currently pending over a piece of software that even the plaintiff described as a "nice feature,"[56] and why hundreds more lawsuits are pending under that statute. It also explains why plaintiffs' lawyers have set up websites to identify and collect potential plaintiffs to sue over privacy and security claims.

Because of the mismatch between the parties that enforcers should go after and whom plaintiffs' attorneys do go after, businesses suffer, and consumers have nothing to show for it.

What Is the Solution?

The best solution is to preclude private rights of action, which are costly for businesses and fail to further the aims of privacy and security laws.

However, for statutes that include an ill-advised private right of action, limiting attorneys' fees is a step in the right direction. Legal standards for attorneys' fees vary across the country and in different types of cases. As policymakers consider privacy and security laws, they should ensure that their states' standards limit excesses and discourage abusive lawsuits.

There are several ways to ensure that attorneys' fees remain reasonable. One is to look to the hours actually spent on the case. A common approach is the "lodestar" method: "the number of hours reasonably expended on the litigation multiplied by a reasonable hourly rate."[57] Numerous statutes require fees to be "reasonable" and require review of awards.[58] Other approaches, like the "common fund" approach that prevails in class actions, permit reasonable percentage-based and contingency fees but subject them to further review[59] where the reasonableness of the percentage should be determined in relation to the amount actually claimed by class members from the fund, not the amount in the fund that is theoretically available to the class. The trend in the federal courts has been to rein in excesses.

Legislators should not usher in an era of jackpot justice and outsized attorneys' fees. Keeping a close watch on fees in emerging privacy and security litigation will help disincentivize economically inefficient and opportunistic litigation and instead focus on true harms to consumers.

How Will This Help Consumers and the Economic Climate?

Capping attorneys' fees will help realign the private incentives of plaintiffs' lawyers to better reflect the public interest. Consumers, as opposed to their lawyers, may also receive a larger payout from a successful lawsuit if fees are based on the amount actually claimed by plaintiffs.

The economic climate will benefit from a more rational allocation of resources by plaintiffs' lawyers against the true bad actors—as opposed to legitimate businesses with deep pockets. And cutting against plaintiffs' lawyers' default incentives to sue will reduce the total volume of litigation.

State Legislation

State privacy and data security legislation should not include private rights of action. However, if and when a private right of action is included in such legislation, the bill should require a "lodestar" approach for attorney compensation or cap attorneys' fees at an enumerated percentage of damages (and in the case of class actions, it should be based on the amount of damages class members actually receive). These provisions appear in a number of different statutes and proposed legislation.

- The Civil Rights Attorney's Fees Award Act of 1976 provides that "*the court, in its discretion*, may allow the prevailing party, other than the United States,

a *reasonable* attorney's fee" when plaintiffs bring suits to enforce several different federal statutes.[60] In applying this statute, courts use the "lodestar" method, multiplying the "number of hours reasonably expended" by "a reasonable hourly rate," with the burden to establish these figures on the party seeking an award.[61]

- Under the Federal Tort Claims Act, "[n]o attorney shall charge, demand, receive, or collect for services rendered, fees in excess of 25 per centum of any judgment rendered pursuant to section 1346(b) of this title or any settlement made pursuant to section 2677 of this title, or in excess of 20 per centum of any award, compromise, or settlement made pursuant to section 2672 of this title."[62]

- State limits on medical malpractice also offer guidance. For example, in Maine, "[i]n an action for professional negligence, the total contingency fee for the plaintiff's attorney or attorneys shall not exceed the following amounts, exclusive of litigation expenses: A. Thirty-three and one-third percent of the first $100,000 of the sum recovered; B. Twenty-five percent of the next $100,000 of the sum recovered; and C. Twenty percent of any amount over $200,000 of the sum recovered."[63]

- Transparency in Private Attorney Contracting (TIPAC) laws generally improve transparency around state hiring of contingency fee counsel. Missouri's TIPAC statute, which is one of the strongest in the nation, limits the amount a private lawyer can receive from a contingency fee agreement with the state and ensures that fees recovered in these contracts are proportional to the total award for damages.[64]

- The Fairness in Class Action Litigation Act (FICALA) limits attorneys' fees in class actions to a percentage of damage awards actually redeemed by the class members.[65]

If state privacy and security legislation contains a private right of action—which it should not—at the very least, it should include caps on attorneys' fees. While prohibiting private rights of action is the best policy, limits on attorneys' fees help to better allocate the resources of plaintiffs' attorneys, which is a boon for both consumers and industry.

"Missouri's TIPAC statute, which is one of the strongest in the nation, limits the amount a private lawyer can receive from a contingency fee agreement with the state and ensures that fees recovered in these contracts are proportional to the total award for damages."

Recommendation 7: Curtail Municipality Litigation

State privacy and security legislation should prohibit enforcement by municipalities.

What Is the Issue?

Municipalities in recent years have been bringing their own enforcement actions, often through outside counsel, to address national policy issues. This troubling model should not be extended to the enforcement of state privacy and security laws.

Generally, litigation to enforce state law is the responsibility of state-wide enforcers. "Municipal suits have a number of significant consequences beyond the outcomes in individual cases. Not least is the threat of upending the balance of state and local power and of usurping the states' role in representing their residents' interests in litigation."[66]

"Traditionally ... the authorities capable of addressing harms to citizens at large were limited and well defined. By contrast, there are over three thousand counties and almost thirty times as many local government entities in the United States."[67]

Some localities empower private counsel to litigate, seek enormous damages, and recover contingency fees, under government authority. Under a contingency fee model, plaintiffs' firms come out on top with consumers far behind. "The suits are ... hugely profitable to the private plaintiffs' firms involved."[68]

Furthermore, incentives are not aligned. "[P]rivate plaintiffs' lawyers' interests in collecting settlement payments for their clients may not fully align with those municipalities' own interests ... Similarly, diverting a public function to private attorneys further undermines the role of statewide elected officials and legislative bodies."[69]

Some proponents of municipality litigation argue that victims benefit when cities recover because they are "closer" to citizens. But municipal public programs may not adequately represent state-wide interests in enforcement of the law, may have different priorities, and may not compensate all victims of privacy violations.

Giving municipalities authority to enforce state privacy and security laws will lead to a jumbled patchwork of intrastate enforcement actions, complicate national

resolution of controversies, and harm consumers. Particularly given the movement of people, data, and services across political boundaries, any enforcement of state privacy and security laws should be the exclusive realm of the state AG.

Why Does This Matter?

FIRST

State AGs—not municipal plaintiffs—are best positioned to protect consumers. State AGs have long been vested with sovereign police power to enforce state law and protect citizens.[70] Municipalities and city officials have traditionally assumed limited roles in consumer protection issues.[71] A shift to more litigious municipalities will usurp the historical ability of AGs to protect all consumers in the state by creating uneven and unpredictable enforcement approaches.

> *"Giving municipalities authority to enforce state privacy and security laws will lead to a jumbled patchwork of intrastate enforcement actions, complicate national resolution of controversies, and harm consumers."*

SECOND

Municipalities' incentives may be skewed to push for enforcement as a way to raise money. Large settlements may be alluring to municipalities facing budget constraints. Local governments may be promised large recoveries with no risk to municipal budgets by contingency fee trial lawyers.

THIRD

Municipality litigation raises political accountability problems. Local government actors—such as municipal attorneys, local council members, and even local executives, especially those who are not elected—may not be as broadly accountable to the public as state legislatures, governors, and AGs.

Worse, there is a growing trend of municipalities using private lawyers on a contingency fee basis.[72] This model outsources the immense power of consumer protection laws to private attorneys with self-interest and little political accountability. Consequential consumer protection decisions should be made by the state AG, not a local actor with narrow interests, or a private attorney seeking a payday.

"Data privacy municipal lawsuits are likely to grow in prominence," and there are already examples by way of suits by Los Angeles against the maker of the Weather Channel mobile app and the City of Chicago after the Marriott data breach.[73] This trend is troubling and risks further fragmenting state law and policy with different approaches and interpretations across

> *Municipal enforcement creates a patchwork within a patchwork. Privacy law is already in danger of balkanization at the state level. Municipal approaches would splinter that even further.*

various localities within a state. This undermines uniformity and unfairly empowers localities like large cities, which may have resources and political or budgetary reasons to bring enforcement actions that might be at odds with the views or priorities of other local leaders or state-wide officials.

FOURTH

Municipal enforcement creates a patchwork within a patchwork. Privacy law is already in danger of balkanization at the state level. Municipal approaches would splinter that even further.

All 50 states have their own breach notification laws,[74] and there are a plethora of state internet privacy laws.[75] The cacophony of laws already on the books makes navigation of the privacy and security landscape confusing for businesses. In a survey conducted by TrustArc, one-fifth of commercial respondents anticipate spending over $1 million to comply with the California Consumer Privacy Act (CCPA).[76] Allowing municipal governments to also pursue actions will make costs skyrocket while creating an unpredictable regulatory and enforcement system within states.

FIFTH

Municipality litigation can stall resolution and divert recoveries away from consumers. "Settlements that achieve the dual aims of addressing plaintiffs' alleged harms while also providing defendants with finality and predictability are much more difficult to achieve" if local governments become involved and have competing or divergent interests.[77] And municipalities divert a considerable share of settlement funds into municipal coffers, rather than to consumers who have been harmed. Although such programs are well-intentioned, they may be inadequate for individuals seeking compensation for their actual injuries.[78]

What Is the Solution?

The answer is simple: states should preclude the ability of municipal governments to enforce statewide privacy and security laws.

How Will This Help Consumers and the Economic Climate?

Limiting enforcement of privacy and security laws to state AGs will give consumers a reliable means of redress for actual injuries and allow businesses to effectively cooperate with states to prevent compliance breakdowns.

- Consumers will benefit from a coherent enforcement strategy implemented by an expert agency. AGs can adequately and fairly represent all state residents, as opposed to only those who live within a city or county. And unlike private attorneys hired by municipal politicians,[79] AGs answer to all state constituents politically and/or publicly.[80]

- Businesses will benefit from a harmonized enforcement environment, rather than defending multiple idiosyncratic local enforcers or trying to predict the legal interpretations of varied municipal lawyers. Although emerging state privacy and security laws present considerable challenges to businesses, companies are better off working with state AGs than dozens or hundreds of local officials to ensure compliance.

State Legislation

Data breach notification and privacy laws should vest enforcement authority exclusively with AGs and should not allow for municipal-level enforcement.

Models of exclusive AG enforcement include:

- Nevada's recently updated online privacy law, which vests enforcement discretion in the Nevada AG.[81]

- Washington's biometric privacy law, which states: "This chapter may be enforced solely by the attorney general under the consumer protection act."[82]

State legislators should curtail the authority of municipal governments to bring enforcement actions for purported violations of state privacy and security laws. Such laws should vest exclusive enforcement power in the state's AG.

Conclusion

The United States needs a unified federal approach to consumer privacy and security issues. But in the absence of action from the U.S. Congress, these proposals for policymakers offer solutions that can help to make state legislation and action work better for consumers and businesses alike.

These bedrock procedural protections have proven successful in other contexts to place reasonable limits on liability and exposure to frivolous lawsuits.

By using them in state legislation, policymakers can avoid the avalanche of negative unintended and collateral consequences that could come from a patchwork, state-by-state approach to protecting consumer privacy and security. Now is the time to build reasonable and practical privacy and security policy.

Endnotes

1 Pam Greenberg, *States Break New Ground on Consumer Privacy Regulation*, The NCSL Blog (June 19, 2019), http://www.ncsl.org/blog/2019/06/19/states-break-new-ground-on-consumer-privacy-regulation.aspx.

2 *Data Privacy*, U.S. Chamber Institute for Legal Reform, https://www.instituteforlegalreform.com/issues/data-privacy.

3 *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits* at 1, 3, U.S. Chamber Institute for Legal Reform (Aug. 2017), https://www.instituteforlegalreform.com/uploads/sites/1/TCPA_Paper_Final.pdf ("*TCPA Litigation Sprawl*").

4 *See Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶¶ 20–22, 40.

5 *Ill-Suited: Private Rights of Action and Privacy Claims* at 10–11, U.S. Chamber Institute for Legal Reform (July 2019), https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf ("*Ill-Suited*").

6 Jeff John Roberts, *Court's Biometrics Ruling Poses Billion Dollar Risk to Facebook, Google*, Fortune (Jan. 28, 2019), https://fortune.com/2019/01/28/facebook-face-scanning-bipa/.

7 *See Ill-Suited* at 6 ("Because of the TCPA, millions of dollars have been diverted to the plaintiffs' bar for calls that were never answered, and for calls and text messages that people want to receive."), 8 ("[Fair Credit Reporting Act] class action lawsuits, often based on mere technical violations, continue to snowball.").

8 *GDP and Personal Income*, U.S. Department of Commerce, Bureau of Economic Analysis (Oct. 29, 2019), http://apps.bea.gov/iTable/iTableHtml.cfm?reqid=51&step=51&isuri=1&table_list=1&series=a#.XYDhCZaCnpg.link.

9 *Employment by major industry sector*, U.S. Department of Labor, Bureau of Labor Statistics (Sep. 4, 2019), https://www.bls.gov/emp/tables/employment-by-major-industry-sector.htm.

10 *Ill-Suited* at 16 ("Unlike litigation trumped up by the plaintiffs' bar to reach a quick payday, enforcement actions at their core are meant to identify and remedy noncompliance that raises concerns for consumer and patient privacy and promote fair competition within industries.").

11 David Sapin et. al., *How consumers see cybersecurity and privacy risks and what to do about it*, PWC (2017), https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html (explaining that 87 percent "of consumers say they will take their business elsewhere if they don't trust a company is handling their data responsibly").

12 Nev. Rev. Stat. Ann. tit. 52, § 603A.360 (2019).

13 *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239 (2012).

14 15 U.S.C. § 2310(e).

15 Minn. Stat. § 363A.331(2).

16 Cal. Civ. Code § 1798.150(b).

17 *Id.* § 1798.155(b).

18 *Model Privacy Legislation*, U.S. Chamber of Commerce (Feb. 13, 2019), https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf ("*Chamber Model Privacy Legislation*").

19 *Black's Law Dictionary*.

20 *Businesses Struggling with GDPR After One Year, Says Thomson Reuters Survey*, Thomson Reuters (May 22, 2019), https://www.thomsonreuters.com/en/press-releases/2019/may/businesses-struggling-with-gdpr-after-one-year-says-thomson-reuters-survey.html.

21 Murat C. Mungan, *Seven Costs of Data Regulation Uncertainty*, Data Catalyst (June 2019), https://datacatalyst.org/reports/what-are-the-costs-of-data-regulation-uncertainty/.

22 Scott Ikeda, *Will New U.S. Privacy Regulations Be Too Expensive for Small Businesses*, CPO Magazine (Mar. 26, 2019), https://www.cpomagazine.com/data-protection/will-new-u-s-privacy-regulations-be-too-expensive-for-small-businesses/.

23 *2019 Small Business Profile*, U.S. Small Business Administration (2019), https://cdn.advocacy.sba.gov/wp-content/uploads/2019/04/23142610/2019-Small-Business-Profiles-States-Territories.pdf.

24 15 U.S.C. § 6503(a).

25 *See COPPA Safe Harbor Program*, FTC, https://www.ftc.gov/safe-harbor-program (last visited Nov. 6, 2019).

26 Ohio Rev. Code Ann. tit. 13, § 1354.02 (2018).

27 *Chamber Model Privacy Legislation*.

28 *Cost of a Data Breach Report 2019*, IBM Security (2019), https://www.ibm.com/security/data-breach.

29 *Consumer Attitudes Towards Data Privacy, IBM-Harris Poll Survey 2019: US Data* at 3, IBM (2019), https://newsroom.ibm.com/download/IBM+Data+Privacy.pdf.

30 *Id.*

31 *See, e.g.,* Sara Salinas, *Facebook stock slides after FTC launches probe of data scandal*, CNBC (Mar. 26, 2018), https://www.cnbc.com/2018/03/26/ftc-confirms-facebook-data-breach-investigation.html.

32 *See* Peter Kafka, *Facebook will pay the US government a $5 billion fine for privacy failures – but it won't have to change the way it does business*, Vox (Jul. 24, 2019, 10:00 A.M.), https://www.vox.com/recode/2019/7/24/20708359/facebook-ftc-settlement-criticism-5-billion-privacy-review-antitrust-mark-zuckerberg (noting that the dissenting FTC Commissioners "are sharply opposed to the settlement because they say it doesn't go nearly far enough").

33 *See TCPA Litigation Sprawl* at 2.

34 William Turley, *How You Can Get Big $$$ For A Winning Unwanted Text or Call Case*, Turley Law Firm P.C., https://www.turleylawfirm.com/library/how-to-win-text-message-lawsuit.cfm (last visited Nov. 6, 2019).

35 *TCPA Litigation Sprawl* at 8.

36 *See The Juggernaut of TCPA Litigation: The Problems with Uncapped Statutory Damages* at 10, U.S. Chamber Institute for Legal Reform (Oct. 2013), https://www.instituteforlegalreform.com/uploads/sites/1/TheJuggernautofTCPALit_WEB.PDF (describing a case in which a small business was found liable under the TCPA after explaining that "statutory damages of $5,524,500 would force its bankruptcy").

37 *GDP and Personal Income*, U.S. Department of Commerce, Bureau of Economic Analysis (Oct. 29, 2019), http://apps.bea.gov/iTable/iTableHtml.cfm?reqid=51&step=51&isuri=1&table_list=1&series=a#.XYDhCZaCnpg.link.

38 42 U.S.C. § 1320d-5(a)(1).

39 *Id.* § 1320d-5(a)(3)(A).

40 *See* W. McDonald Plosser, *United States: Sky's The Limit? A 50-State Survey of Damages Caps And The Collateral Source Rule*, Mondaq (Dec. 11, 2018), http://www.mondaq.com/unitedstates/x/762574/Insurance/Skys+The+Limit+A+50State+Survey+Of+Damages+Caps+ And+The+Collateral+Source+Rule.

41 Ala. Code § 6-11-21(a), (j).

42 *Ex Parte Young*, 209 U.S. 123, 160 (1908).

43 *About NAAG*, National Association of Attorneys General, https://www.naag.org/naag/about_naag.php (last visited Nov. 6, 2019).

44 *See* Cary Silverman & Jonathan L. Wilson, *State Attorney General Enforcement of Unfair or Deceptive Acts and Practices Laws: Emerging Concerns and Solutions*, 65 U. Kan. L. Rev. 209 (2016) ("Consumer protection laws provide state attorneys general (AGs) with sweeping authority to address improper business practices.").

45 *See, e.g., Consumer Tips*, Ohio Attorney General, https://www.ohioattorneygeneral.gov/Individuals-and-Families/Consumers/Consumer-Tips (last visited Nov. 6, 2019); *Filing a Consumer Complaint*, New York Attorney General, https://ag.ny.gov/consumer-frauds/Filing-a-Consumer-Complaint (last visited Nov. 6, 2019).

46 *See, e.g.*, *Protecting Consumers*, State of California Department of Justice, https://www.oag.ca.gov/consumers (last visited Nov. 6, 2019) (offering consumer tips in numerous different categories and recommendations for private attorney referrals).

47 19 Wash. Rev. Code 375.030(2); *see also* Tex. Bus. & Com. Code Ann. § 503.001(d) ("A person who violates this section is subject to a civil penalty of not more than $25,000 for each violation. The attorney general may bring an action to recover the civil penalty.").

48 52 NV Stat. § 603A.360.

49 *Unstable Foundation, Our Broken Class Action System and How to Fix It* at 6, U.S Chamber Institute for Legal Reform (Oct. 2017) https://www.instituteforlegalreform.com/uploads/sites/1/UnstableFoundation_Web_10242017.pdf ("*Unstable Foundation*").

50 *Ill-Suited* at 10–11.

51 *See Inside the Firm: Privacy and Technology*, Edelson, https://edelson.com/inside-the-firm/privacy-and-technology/ (last visited Nov. 6, 2019).

52 Mike Mimoso, *IoT Hacks May Bring Frenzy of Litigation*, Flashpoint Blog (Aug. 21, 2018), https://www.flashpoint-intel.com/blog/iot-hacks-may-bring-frenzy-of-litigation/.

53 Two recent cases, both involving Google, involve settlements with cy pres components. *See, e.g., In re: Google Inc. Cookie Placement Consumer Privacy Legislation*, 934 F.3d 316, 320–21 (3d Cir. 2019) (vacating an order approving a settlement where defendant Google "agreed to stop using the cookies for Safari browsers and to pay $5.5 million to cover class counsel's fees and costs, incentive awards for the named class representatives, and cy pres distributions, without directly compensating any class members"); *Frank v. Gaos*, 139 S. Ct. 1041, 1045 (2019) (concerning a settlement of $8.5 million between plaintiffs and Google, where "[n]one of those funds would be distributed to absent class members," but rather "most of the money would be distributed to six *cy pres* recipients"). Other cases are similar. *See, e.g., In re Baby Prods. Antitrust Litigation*, 708 F.3d 163, 169–70 (3d Cir. 2013) (attorneys requested ~$14 million as a percentage of the $35.5 million settlement, where ~$18.5 million was designated for cy pres and only ~$3 million to consumers); *Dennis v. Kellogg Co.*, 697 F.3d 858, 863 (9th Cir. 2012) (counsel requested ~$2 million in fees from a $10.64 million settlement where $5.5 million went to cy pres and only $800,000 to consumers).

54 Daniel Castro, *Who Stands to Benefit the Most From New Data Privacy Laws? Lawyers*, Information Technology & Innovation Foundation (Aug. 9, 2019), https://itif.org/publications/2019/08/09/who-stands-benefit-most-new-data-privacy-laws-lawyers.

55 *See generally Unstable Foundation*.

56 *See generally Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019).

57 *Hensley v. Eckerhart*, 461 U.S. 424, 433 (1983).

58 *See, e.g.*, 42 U.S.C. § 1988(b).

59 *See, e.g.*, 28 U.S.C. § 2678.

60 42 U.S.C. § 1988(b).

61 *See Hensley*, 461 U.S. at 433.

62 28 U.S.C. § 2678.

63 Me. Rev. Stat. Ann. § 24.2961(1); *see also* Ronald V. Miller Jr., *Limits on Malpractice Fees Around the Country*, Maryland Injury Lawyer Blog, https://www.marylandinjurylawyerblog.com/malpractice-attorney-fees.html (last visited Nov. 6, 2019).

64 *See Missouri Furthers Legal Reform Progress with Transparency in Private Attorney Contracting*, U.S. Chamber Institute for Legal Reform (June 7, 2018), https://www.instituteforlegalreform.com/resource/missouri-furthers-legal-reform-progress-with-transparency-in-private-attorney-contracting.

65 Fairness in Class Action Litigation Act. H.R. 985 (2017).

66 *Mitigating Municipality Litigation: Scope and Solutions*, U.S. Chamber Institute for Legal Reform (March 2019), https://www.instituteforlegalreform.com/uploads/sites/1/Mitigating-Municipality-Litigation-2019-Research.pdf ("*Mitigating Municipality Litigation*").

67 *Id.*

68 *Id.*

69 *Id.*

70 *See Mitigating Municipality Litigation* at 15; *see also Ex Parte Young*, 209 U.S. 123, 160 (1908) (noting that state attorneys general typically have authority to "institute, conduct, and maintain all suits and proceedings ... necessary for the enforcement of the laws of the state ...").

71 *Mitigating Municipality Litigation* at 1, 4.

72 *See id.* at 8.

73 *Id.* at 13.

74 *Security Breach Notification Laws*, National Conference of State Legislatures (Sep. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

75 *State Laws Related to Internet Privacy*, National Conference of State Legislatures (Aug. 13, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

76 Roslyn Layton, *The costs of California's online privacy rules far exceed the benefits*, American Enterprise Institute (Mar. 22, 2019), http://www.aei.org/publication/the-costs-of-californias-online-privacy-rules-far-exceed-the-benefits/.

77 *Mitigating Municipality Litigation* at 15.

78 *See id.* at 16.

79 *See id.* at 8 ("[L]ocal elected leaders may see opportunities for publicity and political gain in taking up causes popular with their backers.").

80 *See id.* at 15.

81 52 NV Stat. § 603A.360.

82 19 Wash. Rev. Code 375.030(2); *see also* Tex. Bus. & Com. Code Ann. § 503.001(d) ("A person who violates this section is subject to a civil penalty of not more than $25,000 for each violation. The attorney general may bring an action to recover the civil penalty.").

Notes

U.S. CHAMBER
Institute for Legal Reform

202.463.5724 main
202.463.5302 fax

1615 H Street, NW
Washington, DC 20062

instituteforlegalreform.com