Insight

A Primer on Data Privacy Enforcement Options

JENNIFER HUDDLESTON | MAY 4, 2020

Executive Summary

- Enforcement options for a federal data privacy law often are presented as a binary choice—either give people the right to sue, or maintain the status quo—but in reality a wide range of options exist.
- There are five general categories of potential enforcement mechanisms that policymakers might consider in various data privacy proposals: 1) a continuation or expansion of enforcement by the Federal Trade Commission (FTC), 2) the creation of a new agency tasked with data protection, 3) enforcement by state attorneys general (typically in combination with federal enforcement), 4) a limited private right of action, and 5) a broad private right of action with monetary relief.
- Policymakers should seek a data privacy enforcement mechanism that allows innovation to flourish by limiting uncertainty while building on the current approach that protects consumers from measurable harm.
- Building on the current FTC-centric regulatory approach, and perhaps supplementing it with assistance from state attorneys general (under specific guidelines), would likely prove effective, while a private right of action or a new agency could create innovation-stifling uncertainty in a number of fields and raise the costs for using such innovations.

Introduction

Since 2018, many involved in technology policy—from privacy advocates to consumers and even tech companies themselves—have called for federal data privacy legislation. Headline-generating events such as the Cambridge Analytica scandal[1] and the resulting concerns about consumers' loss of control over their online data have spurred these calls. Additionally, new international requirements, such as European Union's (EU) General Data Protection Rule (GDPR) and Brazil's General Data Protection Law, have forced many American companies to change their operations, while individual states are passing legislation that will likely create a confusing, patchwork regulatory environment.[2] The privacy-policy landscape has shifted quickly over the last several years, and it is not surprising that many are seeking a federal solution.

One key hurdle to passing federal data-privacy legislation has been the question of how to enforce the any new privacy requirements.[3] The choice has typically been presented as binary: Either individuals have a private right of action—i.e. the ability to sue over privacy infringement—or they do not, and no other options exist. In reality, however, a wide range of options exist. These debates are closely tied to difficulties and concerns regarding what harms a data protection law should seek to address. If additional harms beyond those currently subject to enforcement will be subject to penalty under a new data protection law, these harms should be clearly articulated ito provide clarity for enforcers, consumers, and innovators. The debate over harm is worthy of a fuller discussion beyond the scope of this primer, but an overly broad definition of harm could deter innovation either by creating uncertainty for covered entities or by generating concerns about the potential costs of overly aggressive enforcement.

This primer analyzes the potential benefits and tradeoffs the various approaches to enforcing data protection law as well as why policymakers should be cautious of the potential unintended consequences associated with them.

Enforcement Options and Their Tradeoffs

Existing privacy laws, federal proposals, and state legislation (both successfully passed and proposed) use or have considered using a variety of enforcement mechanisms. For example, proposals in Washington state and New York have included expansive private rights of action, allowing consumer and class-action lawsuits for violations.[4] The current interpretations of the California Consumer Privacy Act include a more limited private right of action that applies only to data breaches.[5] Federal bills have also varied in their preemption of state enforcement and their own methods of enforcement.

There are five categories of potential enforcement mechanisms that are present in various data privacy proposals: 1) a continuation or expansion of Federal Trade Commission (FTC) enforcement, 2) the creation of a new agency tasked with data protection, 3) enforcement by state attorneys general (typically in combination with federal enforcement), 4) a limited private right of action, 5) and a broad private right of action. In determining which approach or combination of approaches to take, policymakers should examine both the potential benefits as well as negative consequences of each approach. Enforcement choices can impact not only the penalties for violating new data protection regulations, and thus the incentives for protecting privacy, but also the overall framework for innovation. The use of these approaches in existing privacy contexts (such as the Children's Online Privacy Protection Act, or COPPA) or state or foreign jurisdictions can provide key evidence of what might happen if applied more broadly to consumer data privacy in the United States.

Continued or Expanded FTC Enforcement

The FTC has been the federal enforcer for various data privacy and security concerns, largely under its unfair and deceptive trade practices authority. This enforcement includes the ability to act for both many specific data privacy laws, such as COPPA, as well as more general concerns.[6] Such an approach has had some key advantages, but there are also concerns about uncertainty and incentives for both consumers and innovators.

While some advocates and officials have criticized the current FTC approach as lacking sufficient deterrence power[7], policymakers should not ignore the success and advantages of the current approach. By focusing on specific *ex post* redress (reviewing the violation and giving fines after it has occurred) rather than a broad *ex ante* approach (scrutinizing all the possible data activities and violations in advance), the FTC does not limit both the direction of innovation and the options available to consumers.[8] *Ex post* redress prevents an overly prescriptive approach that assumes only one set of preferences and presumes to know the ways in which

technology can evolve, but still allows authorities to intervene when necessary to prevent catastrophic or irreversible damage. Europe's GDPR regulation is a good example of a highly prescriptive *ex ante* regulation, and the results have been predictable: Various products, from email management applications to online games, have been unavailable in Europe following the GDPR due to the cost or even impossibility of compliance.

Under its existing authority, the FTC has already taken significant actions regarding data privacy. For example, the agency settlement with Facebook regarding the Cambridge Analytica scandal and stemming from violations of its prior 2012 consent decree resulted in a more sizeable financial penalty than could have been pursued under GDPR.[9] But the agency's current actions are not just limited to such high-profile cases. According to the most recent update released by the agency, the FTC has brought over 130 spam and spyware cases, 80 general privacy cases, 70 data security cases, and 100 cases involving Fair Credit Reporting Act violations**.[10]** The FTC would be able to build on this experience and expertise to provide a balanced approach that both redresses and deters harm while enabling innovative uses of data and wide range of preferences.

While the FTC's current data-privacy approach has prevented an unnecessarily precautionary approach, there are opportunities for reform that could improve on the FTC's enforcement. First, there should be greater certainty around what constitutes a data privacy violation. This uncertainty stems from a lack of clarity around what constitutes a violation and what the FTC could do as an enforcement action. Because most data privacy actions have been settled by consent decree, there is a lack of common law development for innovators to refer to.[11] The length of time these consent decrees (binding settlements between the agency and a company that agrees to certain behaviors but does not admit guilt or establish liability) are enforceable represents significant actions that can be business-ending in the quickly moving world of emerging technology. It is not unusual for consent decrees to last 20 years. Additionally, there are concerns that the agency lacks sufficient personnel and rulemaking resources to enforce a comprehensive data privacy law.[12] For example, FTC Chairman Joe Simons has repeatedly stated in congressional testimony and other official statements that while the FTC does not seek broad rulemaking authority in this area, narrowly tailored rulemaking authority and additional resources in a federal data privacy law would assist in its enforcement.[13] Many of these concerns could be addressed in any federal data privacy policy, and such reforms could improve on the existing model.

If policymakers continue the current model that has largely allowed innovation to flourish by selecting FTC enforcement for any data protection policy, they should also consider potential reforms that could help remedy some of the current disadvantages.

First, there should be clarity around what constitutes violations. As former FTC chief technologist Neil Chilson points out, privacy legislation provides lawmakers an opportunity to clarify for innovators and regulators what exactly the FTC's Section 5 authority is. (Section 5 authority refers to the section of the FTC Act that grants the agency broad enforcement authority over "unfair or deceptive trade practices affecting commerce."[14] The FTC has previously issued statements clarifying and defining what constitutes an unfair or deceptive practice. [15]) Any such legislation, however, should focus on clarifying the criteria for injury and proportional responses rather than codifying a static view of best practices.[16] A more context-specific policy statement regarding what constitutes a violation in the rapidly evolving field of data usage would provide greater clarity and certainty for both consumers and innovators. This statement is particularly important in establishing[17] an actionable violation of new data protection or existing consumer protection law.[18]

Second, policymakers could grant limited additional rulemaking authority in this area. This authority should reflect the clarified standards of authority and be accompanied by clear guidelines regarding its uses. This clarity is necessary to limit the overregulation concerns and agency overreach that took place in the 1970s prior to the creation of the modern unfairness test,[19] which was established in the 1980s and codified in 1994.

Under this test, a practice is considered unfair only if it involves a substantial injury, lacks off-setting benefits, and cannot be reasonably avoided by consumers.[20] This clarity has been used in existing data-privacy laws such as COPPA where the FTC has been granted specific enforcement. If the FTC is to receive additional enforcement or rulemaking authority, legislators should provide clear delegation of the specific areas of data protection to be addressed through these actions. Such clarity would also help to prevent potential conflicts resulting from overlapping authority with other agencies such as the Federal Communications Commission.[21]

Finally, any additional expectations should be accompanied by the appropriate resources for staffing and enforcement. In some cases, this could be accomplished by assistance in enforcement by state attorneys general or through cooperation with other agencies such as the Department of Justice.

Creation of a New Data Protection Agency

Some have advocated that a new data protection law in the United States should include the creation of a new agency for oversight and enforcement, similar to what many European countries have done. Some federal legislative proposals, such as Senator Kirsten Gillibrand's Data Protection Act, have proposed a similar agency in the United States that would enforce data protection law and related issues rather than the FTC.[22]

Those in favor of a new agency point to the ability of a new agency to develop specific expertise that may be lacking in the current enforcement regime.[23] Additionally, advocates argue a new agency would be able to regulate data comprehensively instead of being constrained by pre-existing areas of focus. Such an agency, for example, could regulate not only data privacy and security concerns but also the broader use of data in many rapidly emerging areas, such as artificial intelligence or big data, that might fall outside the purview of current agencies.[24]Yet, there are tradeoffs to such an approach, and many of these benefits could be achieved in other ways. A new data protection agency could create a significant expansion of the administrative state, and once created, it could be difficult to curtail the power of such an agency, as data usage touches nearly every aspect of the economy.

Moreover, there may be existing agencies, such as the FTC, that already have the necessary expertise on specific data issues as well as the experience in responding to consumer harms and concerns—and such combined expertise would be particularly helpful for regulating data. Enforcement actions should be based on specific economic or other legally recognized harm instead of just statutory violations without specific injury. A new agency focused only on data may be less likely to look at the interactions and tradeoffs involved in regulating data privacy and might not have the expertise to look at damages beyond the data itself. Specialized European data agencies, for example, have been active, but it is less clear that privacy and security have improved as a result.[25]

Additionally, the creation of a new agency raises questions about its structure. Data privacy is a politically fraught area, and the desire to create a capable agency could lead lawmakers to structure it in ways that insulate it from political pressures. The desire to solve a problem may not lead to clarity around authority and could undermine necessary checks and balances, as has been seen in the ongoing legal battles over the Consumer Financial Protection Bureau.[26]

While a new agency to handle enforcement of data protection has benefits, most of the advantages could be achieved by reforming, clarifying, and expanding the existing authority of the FTC rather than further growing the administrative state. Rather than creating a new agency, policymakers should look to achieve similar benefits by leveraging existing expertise and providing more resources where needed.

Enforcement by State Attorneys General

Some policymakers have noted that the federal government faces resource constraints in any new enforcement endeavor, and they have also highlighted some benefits of state involvement in data protection. As a result, some federal data-protection proposals, including the discussion draft of Senate Commerce Committee Chairman Roger Wicker's United States Consumer Data Privacy Act, have proposed that state attorneys general serve as enforcers of federal data privacy law.

This approach to enforcement has a few advantages. First, it expands resources for enforcement beyond those currently available at federal regulatory agencies. Additionally, the use of state attorneys general could shift enforcement away from the issues of the "common law of consent decree" to a truer common law approach. The current approach relies heavily on consent decrees rather than establishing precedent through litigation and the courts. This method can make it difficult to determine the relevant precedent and whether certain actions are violations, creating confusion. Critics have pointed out that the current approach mimics the common law in some ways, but without providing the certainty and notice that court precedents could provide.[27] Placing enforcement authority with state attorneys general could require cooperation among states in multistate actions, limiting the number of suits and consolidating the areas of dispute, and could result in more cases going to court, helping to establish precedent. Enforcement actions in the courts could establish precedents that provide greater certainty than the current "common law of consent decrees" and provide a check on administrative authority, preventing overreach.

A key benefit of a federal data protection law would be that it would prevent a patchwork of state privacy laws from disrupting innovation. Federal policymakers need to carefully consider if enforcement by state attorneys general risks undermining this benefit, as a plethora of interpretations could result in a non-uniform and potentially disruptive patchwork itself.[28], [29] Additionally, one state's overly restrictive or narrower interpretation could potentially disrupt the intended solution or policy.[30] There is also the risk that allowing state litigation could open the floodgates to industry-crushing litigation.

Other areas of consumer protection law, however, show that a balanced approach is possible. For example, state attorneys general already engage in enforcement actions on a variety of consumer protection issues as well as antitrust, including actions regarding data breaches and a variety of other technology-related consumer concerns.[31] In a federal data privacy law, any delegation of this power should have clear federal guidance on enforcement and interpretations to prevent a single state attorney general from disrupting a federal framework. With such guidelines, states could be part of the federal solution to concerns about data protection enforcement.

Private Right of Action

Some privacy advocates have suggested that any data protection law needs a private right of action, in which individuals and classes of consumers would be able to sue for violations of data privacy law. Such enforcement has been included in proposals from states including New York and Massachusetts, as well as some federal proposals from Senate Democrats, including Senator Maria Cantwell's Consumer Online Privacy Rights Act.[32] Proponents of a private right of action argue that it provides access to remedies for those harmed, enables

enforcement despite agency resource limitations, and creates stronger incentives for compliance with privacy legislation.[33]

A private right of action, however, has many disadvantages that could limit innovative options, including innovations that might improve privacy and security, due to concerns about liability.[34] Some of these concerns regarding the lack of a loser-pays rule and high cost of litigation, about an explosion in litigation, and about high attorneys' fees with significantly smaller payouts to harmed plaintiffs are not limited to data protection but have been discussed in the broader context of needs for tort reform. In general, a private right of action would not ensure that remedies appropriately addressed privacy harms. Particularly in an area such as privacy law where alleged harms are often amorphous and difficult to measure, such an enforcement mechanism is likely to create more potential problems than it solves. As a result, the potential consequences and pitfalls of a private right of action have been a concern across the political spectrum, from libertarians to liberals. The Obama Administration's Privacy Bill of Rights expressly stated that such legislation would not grant a private right of action for enforcement.[35] Similarly, many of the existing data privacy laws in sensitive areas including health care and financial information are enforced without a private right of action.[36]

A private right of action for enforcement could involve injunctive relief with or without the addition of monetary sanctions. Many of the potential issues with a private right of action stem from the incentives provided by the potential for monetary relief. A narrow private right of action that only offered injunctive relief would have fewer incentives for the potential abuses associated with the broader tort system. Still, without clearly defined harms in legislation or by delegated authority, there is potential that a large amount of litigation, even under such a narrow private right of action, could deter not only harmful actions but creative ideas that have unknown levels of risk at the time. Investors might still be concerned about the uncertainty of new ideas and products that could be delayed by private litigation, even if they seem allowed initially. Litigation in and of itself is expensive, and allowing a private right of action could result in such expenses that could bankrupt a company even if it ultimately defends against the claim.[37]

More concerning are calls for a broad private right of action that would include monetary relief. Such a private right of action is used to enforce Illinois' Biometric Information Privacy Act (BIPA) and has had significant consequences. For example, because of BIPA's enforceability through litigation, certain products such as phototagging options are not available in the state as companies may seek to avoid increased liability risks, and employers may find themselves subject to suits for deploying more secure time-keeping technologies.[38] The increased risk of litigation from potential per se violations that are not related to clearly identifiable harms are not just a burden on large companies. Such an enforcement mechanism also raises compliance costs and liability risks for employers seeking to use better security measures, such as fingerprint clock-ins or amusement parks trying to ensure the same person always uses an annual pass.[39] These potential risks of innovative uses of data where monetary rewards are available are only further exacerbated if the harm is not clearly defined. For example, the Ninth Circuit held that mere collection of biometric data without sufficient consent was a sufficient harm to allow a class action to proceed.[40] State courts in Illinois have found that it is not necessary for an actual harm to have occurred for a lawsuit to be brought under BIPA, allowing for even more potential litigation.[41] The risks in such a situation can easily outweigh the benefits of innovation. In contrast, Texas and Washington have biometric privacy laws that lack a private right of action. Such an approach still enables enforcement and protection for what has been deemed more sensitive information but prevents many of the pitfalls associated with a private right of action.

Given the intangible nature of many alleged privacy harms, a private right of action over data privacy would only further exacerbate the more general concerns about class actions and the American tort system. Since each individual harm in data privacy is likely to be very small, most of these cases would probably be brought as

class actions. In many class-action cases, when successful, the resulting award results in large amounts for the attorneys that argued the case, but the actual payments to the class involved can be rather small or even go to a selected non-profit instead due to difficulties in identifying class members.[42] Additionally, the lack of a "loser-pays" rule can result in misaligned cases of questionable merits that can still lead to settlements out of concerns about the cost and uncertainty of litigation as well as the potential public perception of arguing against such a claim.[43] As data touches almost every aspect of the economy, a broad private right of action would only increase the frequency of these claims and liability for a wide range of industries.

Given the significant consequences of a private right of action, policymakers should be hesitant about including such an enforcement mechanism. If any private right of action is included, one limited to injunctive relief has less incentives for potential overuse or abuse.

Conclusion

Enforcement should be among the specifics that need to be carefully considered by policymakers approaching data protection policy in the United States. Policymakers should ensure that enforcement options do not undermine the framework that has allowed the United States to be a leader in innovating many beneficial applications of data. The current regulatory regime is largely a permissionless model that focuses on tangible harms and allows a wide range of preferences. When examining the potential tradeoffs associated with various enforcement options, the choice that minimizes unintended consequences is the one that improves on this model.

To this end, policymakers should first continue the current FTC-centric approach and examine potential reforms to improve it. If additional enforcement resources are needed, utilizing state attorneys general with clear guidance along with federal enforcement could help solve concerns about resource limitations. The significant tradeoffs of a private right of action or a new agency as well as the unpredictability of their enforcement means policymakers should be cautious about such options. The privacy enforcement debate is not a dichotomy between the status quo and private right of action, but a range of options that policymakers can consider assembling to resolve the disadvantages of each approach on its own.

[1] *See* Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram*, Vox, May 2, 2018, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

[2] **Jennifer Huddleston and Ian Adams "Potential Constitutional Conflicts in State and Local Data Privacy Regulations", released by the Regulatory Transparency Project of the Federalist Society, December 2, 2019 (https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf)**

[3] *See*, *e.g.*, Makena Kelly, *Congress is Split Over Your Right to Sue Facebook*, The Verge, Dec. 3, 2019, https://www.theverge.com/2019/12/3/20993680/facebook-google-private-right-of-action-sue-data-malpractice-wicker-cantwell.

[4] Megan Herr et al., *Washington Privacy Act Update: Private Right of Action Added in the House*, Security, Mar. 4, 2020, https://www.securitymagazine.com/articles/91834-washington-privacy-act-update-private-right-of-action-added-in-house; Kathryn Lundstrom, *New York's Privacy Bill Failed Last Session – But It Gives Us a Look at What Future Laws Might Look Like*, AdWeek, Feb. 21, 2020, https://www.adweek.com/digital/new-yorks-privacy-bill-failed-last-session-but-it-gives-us-a-look-at-what-future-laws-might-look-like/.

[5] Morgan Lewis, *Preparing for the CCPA Private Right of Action for Certain Security Incidents*, JD Supra, Jan. 6, 2020, https://www.jdsupra.com/legalnews/preparing-for-the-traddd-private-right-of-12835/.

[6] *Protecting Consumer Privacy and Security*, Fed. Trade Commission, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security.

[7] *E.g.*, Dianne Bartz, Senators Criticize FTC's Reported Facebook Settlement, Reuters, Jul. 16, 2019, https://www.reuters.com/article/us-usa-facebook-ftc/senators-criticize-ftcs-reported-facebook-settlement-idUSKCN1UB25O

[8] *See* Adam Thierer, *Permissionless Innovation*, at 26.

[9] *See* Josephine Wolff, *The FTC's Remarkable $5 Billion Fine for Facebook*, Slate, Jul. 23, 2019, https://slate.com/technology/2019/07/ftc-facebook-cambridge-analytica-equifax-fines.html.

[10] *Privacy and Data Security: 2019 Update*, Federal Trade Commission, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf.

[11] *See* Jennifer Huddleston, *Unprecedent: The Issue of Agency Action by Consent Order*, Plain Text, Sept. 22, 2017, https://readplaintext.com/unprecedented-the-issue-of-agency-action-by-consent-order-on-innovation-b23ab7b09f42.

[12] *See* Chris Jay Hoofnagle, Woody Hartzog, and Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, But Not Without Help from Congress*, Brookings, Aug. 8, 2019, https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/.

[13] Dennis Fisher, *FTC Pushes for Federal Privacy Law*, Decipher, May 9, 2019, https://duo.com/decipher/ftc-pushes-for-federal-privacy-law.

[14] A Brief Overview of Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority, Federal Trade Commission, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[15] *Id*.

[16] Neil Chilson, "When Considering Federal Privacy Legislation", released by the Regulatory Transparency Project of the Federalist Society, December 4, 2018 (https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper-Privacy-Legislation.pdf).

[18] *See id*.

[19] *See* J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, May 30, 2003, https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

[20] *Id*.

[21] Jennifer Huddleston & Andrea O'Sullivan, *New GAO Report Says It's Time for Federal Data Privacy Legislation. But What Kind?*, The Bridge, Feb. 25, 2019, https://www.mercatus.org/bridge/commentary/new-gao-report-says-its-time-federal-data-privacy-legislation-what-kind

[22] Zach Whittaker, *A New Senate Bill Would Create a US Data Protection Agency*, TechCrunch, Feb. 13, 2020, https://techcrunch.com/2020/02/13/gilliband-law-data-agency/.

[23] *See The U.S. Urgently Needs a Data Protection Agency*, Electronic Privacy Information Center, https://epic.org/dpa/.

[24] *See id*.

[25] *See, e.g.*, Stephanie Hare, *These New Rules Were Meant to Protect Our Privacy. They Don't.*, The Guardian, Nov. 10, 2019, https://www.theguardian.com/commentisfree/2019/nov/10/these-new-rules-were-meant-to-protect-our-privacy-they-dont-work.

[26] *See* Iain Murray, *The Case Against the Consumer Financial Protection Bureau*, Competitive Enterprise Institute, Sept. 21, 2017, https://cei.org/content/case-against-cfpb (discussing issues with CFPB).

[27] *See* Ryan Hageman, Jennifer Huddleston Skees, & Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 17 Colo. L. & Tech. J. 37, 101-3 (2019).

[28] *See* Roslyn Layton, *Never-Ending Net Neutrality Litigation Means Lawyers Always Win*, AEIdeas, Oct. 9, 2019, https://www.aei.org/technology-and-innovation/never-ending-net-neutrality-litigation-means-lawyers-always-win/ (discussing state attorneys general efforts to undermine the Restoring Internet Freedom Order through their own litigation).

[29] *See* Huddleston & Adams, *supra* note 2 at 8-9 (discussing how different interpretations of even similar state laws could create a patchwork of privacy laws).

[30] *See* Jennifer Huddleston, *Gray Areas in States and Local Tech Regulation*, Oct. 16, 2018, The Bridge, https://www.mercatus.org/bridge/commentary/gray-areas-states-and-local-tech-regulation (discussing how states can become de facto national regulators).

[31] *See* Tony Romm, *Facebook, Google Face Off Against a Formidable New Foe: State Attorneys General*, Sept. 8, 2019, https://www.washingtonpost.com/technology/2019/09/08/facebook-google-face-off-against-formidable-new-foe-state-attorneys-general/.

[32] S. 2968, Consumer Online Privacy Rights Act, https://www.congress.gov/bill/116th-congress/senate-bill/2968/text

.

[33] *See, e.g.*, Adam Schwartz, *You Should Have the Right to Sue Companies that Violate Your Privacy*, Electronic Frontier Foundation, Jan. 7, 2019, https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy.

[34] *See Ill-Suited: Private Rights of Action and Privacy Claims*, U.S. Chamber Institute for Legal Reform, July 2019, https://www.instituteforlegalreform.com/uploads/sites/1/Private_Rights_of_Action_-_Ill_Suited_Paper.pdf.

[35] Alan McQuinn & Daniel Castro, *A Grand Bargain on Data Privacy Legislation for America*, Information Technology & Innovation Foundation, January 2019, 61, http://www2.itif.org/2019-grand-bargain-privacy.pdf

[36] *Id*.

[37] *See The Ninth Circuit Clarifies Safe Harbor Rules in Veoh Victory*, https://www.orrick.com/Insights/2013/03/The-Ninth-Circuit-Clarifies-Safe-Harbor-Rules-in-Veoh-Victory (noting that despite its victory the lawsuit regarding a copyright claim against online material appears to be one of the primary causes of Veoh's bankruptcy); *see also* Evan Engstrom, *What is the Value of Section 230?*, Engine, Jan. 31, 2019, https://www.engine.is/news/primer/section230costs (discussing the cost of litigation in context of user generated content for startups, but such information shows that litigation in the united states is a high risk proposition even if a company ultimately wins).

[38] Jennifer Huddleston, *Three Lessons from BIPA for Data Privacy Legislation*, The Hill, Feb. 6, 2020, https://thehill.com/opinion/cybersecurity/481709-three-lessons-from-bipa-for-data-privacy-legislation.

[39] *See* Scott M. Gilbert, *The Eyes are the Window to the Soul…and Liquidated Damages: Illinois Supreme Court Raises the Stakes on Employer Use of Biometric Data*, National Law Review, Jan. 28, 2019, https://www.natlawreview.com/article/eyes-are-window-to-soul-and-liquidated-damages-illinois-supreme-court-raises-stakes; Jon Fingas, *Illinois Biometric Privacy Law Passes a Key Court Test*, Endgadget, Jan. 26, 2019, https://www.engadget.com/2019-01-26-illinois-biometric-privacy-law-passes-a-key-test-in-court.html

[40] Patel v. Facebook, No. 18-15982 (9th Cir. 2019).

[41] Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186.

[42] *Do Class Actions Benefit Class Members?*, Institute for Legal Reform, Dec. 11, 2013, https://www.instituteforlegalreform.com/uploads/sites/1/Class-Action-Study.pdf.

[43] *See* Marie Gryphon, *Greater Justice, Lower Cost: How a "Loser Pays" Rule Would Improve the American Legal System*, Manhattan Institute, Dec. 1, 2008, https://www.manhattan-institute.org/html/greater-justice-lower-cost-how-loser-pays-rule-would-improve-american-legal-system-5891.html