FREE STATE FSF FOUNDATION

Perspectives from FSF Scholars
January 21, 2020
Vol. 15, No. 4

A Privacy Private Right of Action Is Inferior to FTC Enforcement

by

Andrew Long *

I. Introduction and Summary

The new year brings with it a new era in online privacy regulation as companies struggle to define and achieve compliance under the now-effective California Consumer Privacy Act ("CCPA"). In light of the CCPA, as well as the prospect of legislative action by other states, Congress faces ever-increasing pressure to pass a federal law – ideally one that preempts a "patchwork" of state measures.

A point of contention apparently standing in the way of bipartisan agreement is whether that legislation should include a "private right of action" authorizing individuals – on their own or as members of a class – to go to court to seek redress. At one end of the spectrum, proposed legislation would empower consumers to sue for the violation of any statutory provision or implementing rule – and by definition prevail without a requirement to demonstrate actual harm. At the other, the right to bring a legal action would fall exclusively to government entities.

Broadly speaking, enforcement mechanisms ideally serve a number of laudable purposes, including the following: creating incentives to engage in conduct that advances policy

objectives and to avoid behavior that leads to identified harms; ensuring that those who fail to comply with legal obligations are not thereby enriched; further refining and clarifying aspirational, *ex ante* legislative guidance through decisions that embrace real-world fact patterns; striking the appropriate balance between protecting consumer interests and allowing the marketplace to operate efficiently; and making those who have been injured whole.

Where they are not calibrated in a proper fashion, however, enforcement tools can produce unintended and negative consequences that lead to a reduction in overall consumer welfare. Penalties that are too high can lead to suboptimal levels of innovation, marketplace participation, and risk assumption, while those that are too low may be disregarded as mere costs of doing business. Provisions that allow for inconsistent, jurisdiction-specific outcomes undermine the refined guidance that national actors might otherwise receive. And the possibility of an unjustified financial windfall can result in the abuse of judicial remedies.

Privacy enforcement, in particular, is vulnerable to such concerns. Infringements upon privacy interests can go undetected, and even when discovered may be impossible to source. In addition, actual damages resulting from violations of individual privacy rights often are difficult to calculate. As a consequence, a private right of action founded on economic injury may not provide consumers the relief that lawmakers intend. Attempted fixes, such as the establishment of statutory (*i.e.*, liquidated) damages, frequently benefit plaintiffs' attorneys more than injured individuals. This especially is true in the case of class actions, which create even greater financial incentives for lawyers to pursue unjustified litigation than do individual suits – and, therefore, cause even greater harm to overall consumer welfare.

A better approach would be to formalize and make exclusive the FTC's enforcement authority. State attorneys general could have a role, as well. Federal legislation that provides the FTC with greater resources, the ability to impose fines for first-time violations, and the authority to compensate victims directly would serve the objectives of privacy oversight well. Specifically, such a law would safeguard consumer online privacy, define clear, nationwide rules of the road for both businesses and consumers, allow oversight to keep up with marketplace developments through a case-by-case, fact-intensive approach, and align litigation decisions with the achievement of sound policy-driven outcomes. And it would do so while still providing aggrieved consumers with the opportunity to receive compensation.

II. A Private Right of Action Is a Crude Tool to Achieve Privacy-Related Goals

In order for rights to have meaning they must be enforceable. Setting aside the issue of what specific privacy rights federal legislation might enumerate (*e.g.*, the right to know, the right to delete, etc.), the question becomes how best to ensure that enforcement mechanisms further the policy objectives that underlie those rights.

Ideally, enforcement motivates businesses to comply with legal obligations, punishes those that do not, provides clarifying guidance to similarly situated entities, and makes injured consumers whole. In other words, it provides businesses with the proper incentives to behave in ways that policymakers prescribe and discourages them from engaging in activities that policymakers prohibit, while also compensating individuals who have been injured as a consequence. In addition, when penalties are tailored carefully, and dispensed in predictable ways, they do not unreasonably interfere with the efficient operation of the marketplace.

Penalties that are too high, or are handed out in unforeseeable and arbitrary ways, create risk and uncertainty. Penalties that are too low, meanwhile, may be dismissed as no more than a manageable expense.

With respect to online privacy specifically, consumers benefit most from measures that strike the proper balance between individual interests and the continued viability of data-driven offerings. Where consumer rights are not enforced adequately, there is the possibility that they will not be honored. And where enforcement goes too far, the resulting risk, uncertainty, and expense may discourage businesses from providing the "free" (ad-supported) content and services that consumers value.

A private right of action is one possible way to drive enforcement – but it is problematic. The Consumer Online Privacy Rights Act ("COPRA"), introduced in late November 2019 by Democratic members of the Senate Commerce Committee Maria Cantwell (WA), Brian Schatz (HI), Amy Klobuchar (MN), and Ed Markey (MA), wholly embraces such an approach. COPRA expressly would empower "[a]ny individual alleging a violation of this Act or a regulation promulgated under this Act [to] bring a civil action in any court of competent jurisdiction, State or Federal."[1] Similarly, the Online Privacy Act of 2019, introduced earlier in November by Zoe Lofgren and Anna Eshoo, Democratic House members representing Silicon Valley, would allow "a person who is aggrieved by a violation of this Act [to] bring a civil action for damages in any court of competent jurisdiction in any State or in an appropriate district court."[2]

In theory, self-interested individuals are well situated to identify instances in which they have experienced harm and the extent of those injuries. In theory, then, it might follow that enabling consumers to initiate judicial action on their own behalf would lead to favored outcomes. But in practice, the inescapably inchoate nature of privacy interests unduly complicates this process. Consumers often are not aware that a privacy violation – say, the display of personal information on a rogue website, or its transfer to an unauthorized third party – has occurred. And even when they are, given the number of businesses with which they choose to share their information, it may be impossible for them to prove with certainty from which specific business that information came.[3]

Moreover, in order to prevail in court, a consumer must be able to demonstrate quantifiable harm. As the U.S. Chamber Institute for Legal Reform has explained, however, "[m]ost courts have recognized … that loss of value of [personally identifiable information] is insufficient to serve as Article III injury under the Supreme Court's guidance in *Spokeo v. Robins* or is

[1] Consumer Online Privacy Rights Act § 301(c)(1) (November 26, 2019), available at https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf (*COPRA*).
[2] Online Privacy Act of 2019 § 407(b) (November 5, 2019), available at https://eshoo.house.gov/wp-content/uploads/2019/11/Bill-Text-Online-Privacy-Act-Eshoo-Lofgren.pdf (*OPA*).
[3] *See, e.g.*, U.S. Chamber Institute for Legal Reform, "Ill-Suited: Private Rights of Action and Privacy Claims" (July 2019), available at https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf, at 2 (arguing that "[w]hen it comes to privacy interests, … the wrongdoer(s) is or are often unknown or unidentifiable").

insufficient injury under the causes of action presented."[4] This significantly undermines the utility of private litigation as a means to advance privacy-related goals.

In addition, an individual private right of action may produce unintended consequences that undermine the policies that enforcement is intended to achieve. The reason for this is straightforward: money. (The root of all evil, indeed.) The possibility of a financial windfall can distort the incentives of individuals, and the attorneys who represent them, resulting in too many lawsuits that serve not to advance the objectives of privacy legislation, but rather to obtain a potential payout.[5]

Importantly, the ability to file class-action lawsuits exacerbates these negative effects. Class actions create even greater incentives for plaintiffs' attorneys, as larger, more far-reaching cases hold open the possibility of bigger judgments or settlements and higher attorney's fees. Meanwhile, individual consumers alleging harm included within the class frequently receive little compensation (*e.g.*, small monetary amounts or vouchers). More often, they receive nothing, yet are bound by the settlement.

Excessive litigation leads to a number of harmful results. One, it unreasonably burdens the taxpayer-funded judicial system, resulting in deferred justice for others. Two, it empowers plaintiffs' attorneys incentivized by financial concerns, not the privacy interests of the general public, to drive the evolution of policy via case law. As the U.S. Chamber Institute for Legal Reform has explained, "[u]nlike litigation trumped up by the plaintiffs' bar to reach a quick payday, enforcement actions at their core are meant to identify and remedy noncompliance … and promote fair competition within industries."[6] Three, district-by-district decisions threaten inconsistent outcomes that create confusion for consumers and force businesses with national footprints – the rule, rather than the exception, for those operating online – to expend limited resources on multiple jurisdiction-specific compliance efforts.

Such lawsuits also subject both actual and potential marketplace participants to increased risk and uncertainty. Risk and uncertainty, in turn, lead to a reduction in overall consumer welfare. Existing businesses may be forced to reallocate resources away from uses that benefit consumers toward legal fees, settlements, and judgments, while potential competitors must consider those additional costs when making market-entry decisions. Providers of "free" (ad-supported) content and services in particular may be sensitive to the threat of such costs. As a consequence, they rationally may choose to discontinue such offerings or implement charges,

---

[4] *Id*. at 2; *see also id*. at 2-4 (citing *Mount v. PulsePoint, Inc.*, 2016 WL 5080131 (S.D.N.Y. August 17, 2016) and *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532 (C.D. Cal. April 28, 2011), concluding that these cases "demonstrate how intangible the 'harms' are in many privacy cases," and noting that "they are not alone in rejecting plaintiffs' 'harm' allegations").

[5] *See, e.g.*, David R. Kott *et al*., "TCPA: The Next Wave of Class Action Lawsuits Asserts Consumer's Right to Withdraw Consent to Receive Text Messages," *Lexology* (February 14, 2017), available at https://www.lexology.com/library/detail.aspx?g=b190ede8-d150-49fe-a591-53241ea0bc11 ("It is important to understand who is on the other side of a [Telephone Consumer Protection Act] claim. These lawsuits have traditionally been brought by the organized plaintiffs' bar. Certain plaintiffs' firms are in the business of investigating (and, in some cases, arguably manufacturing) claims in order to secure a quick payday under the Act.").

[6] U.S. Chamber Institute for Legal Reform, "Ill-Suited: Private Rights of Action and Privacy Claims" (July 2019), available at https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf, at 16.

resulting in consumers having to switch to alternative sources and/or pay for that which they enjoyed previously at no cost. Innovation likely will decrease, as well. Research and development budgets may suffer, and businesses may be less willing to experiment using innovative business models and cutting-edge technologies. Finally, excessive potential liabilities, and legal expenses generally, disproportionately impact smaller entities, which in many cases are new market entrants and, thus, potential future sources of beneficial competition to entrenched and dominant players.

III. Legislative Attempts to Cure These Deficiencies Inevitably Create More Problems

Through the drafting process, lawmakers have sought to craft workarounds for a private right of action's inherent inability to align well with the policy objectives of privacy oversight. Experience demonstrates, however, that efforts to eliminate such infirmities rarely succeed.

Statutory (*i.e.*, liquidated) damages, the most common example, endeavor to sidestep the difficulties surrounding the quantification of privacy interests and injuries thereto by eliminating altogether the requirement to demonstrate actual harm. COPRA's proposed language offers an extreme version of this: Section 301(c)(3) declares that any "violation of this Act or a regulation promulgated under this Act with respect to the covered data of an individual constitutes a concrete and particularized injury in fact to that individual."[7]

The Telephone Consumer Privacy Act ("TCPA")[8] provides decades of data on the practical effects of a statutory damages provision. That history demonstrates how "no-injury" remedies, compounded by the opportunity to pursue class-action litigation, reduce consumer welfare by redirecting capital away from productive uses toward legal fees – and largely result in the transfer of wealth to the plaintiffs' bar. As one commenter has explained, "[t]he TCPA has become fertile ground for nuisance lawsuits because class action lawyers are often rewarded with quick settlements, even in cases without any merit, simply because litigation uncertainty and the potential financial exposure resulting from a bad decision are too great a risk for a company to bear."[9]

---

[7] *COPRA* § 301(c)(3).

[8] 47 U.S.C. § 227. The TCPA's private right of action provides for the recovery of actual monetary loss or statutory damages in the amount of $500 per violation (*i.e.*, unsolicited telephone solicitation), whichever is greater, as well as statutory damages up to $1,500 for every violation that is willful or knowing. *See* §§ 227(b)(3)(B), (C).

[9] Monica Desai *et al*., "A TCPA for the 21st Century: Why TCPA Lawsuits Are On the Rise and What the FCC Should Do About It," *International Journal of Mobile Marketing*, Vol. 8, No. 1 (Summer 2013), at 75-76, available at https://www.squirepattonboggs.com/-/media/files/insights/publications/2014/07/a-tcpa-for-the-21st-century/atcpaforthe21stcentury.pdf. *See also* Megan Brown & Boyd Garriott, "Illinois: Actual Injury Not Required for Privacy Lawsuit; Inviting Costly Litigation against Innovators," *WileyConnect* (January 25, 2019), available at https://www.wileyconnect.com/home/2019/1/25/illinois-actual-injury-not-required-for-privacy-lawsuit-inviting-costly-litigation-against-innovators ("Legions of 'unharmed plaintiffs' and 'injury-free class actions,' encouraged by judges unwilling to enforce standing requirements, pose several unfortunate consequences. They will plague the courts, force companies into massive payouts to plaintiffs' lawyers, and deter technological innovation. States and the U.S. Supreme Court should carefully enforce Article III standing requirements, and legislators considering new privacy laws should be wary of authorizing similar 'harm-free' class actions.").

The proposed Online Privacy Act, meanwhile, tries to mitigate the potential exploitation of class actions by plaintiffs' attorneys through a requirement that such lawsuits be filed only by "a nonprofit body, organization, or association which has been properly constituted in accordance with the law, has statutory objectives which are in the public interest, and is active in the field of the protection of individual rights and freedoms with regard to the protection of their personal data."[10] Though well-intentioned, odds are that this provision will not prevent unwanted class litigation, but rather motivate "creative" workarounds. After all, it is not hard to imagine how a clever and financially motivated attorney might go about establishing a legal entity that checks all of these boxes solely and specifically to thwart lawmakers' objectives.

Such concerns are by no means purely theoretical. The history of the FCC's "designated entity" program well illustrates how this can play out in practice. The goal of the designated entity program is to encourage, through financial incentives, the participation in spectrum auctions of small businesses owned by minorities and women. Tailored definitions strive to limit these advantages to their intended recipients, but not surprisingly other auction participants have sought to identify and exploit ambiguous language and other loopholes for economic gain. In one high-profile example from 2015, Dish Network Corporation, a Fortune 250 company,[11] laid claim to a 25 percent discount for a "very small business" in the Advanced Wireless Services (AWS-3) auction through a carefully constructed web of corporate entanglements including a partnership with an Alaska Native regional corporation.[12] (Pursuant to the Alaska Native Claims Settlement Act, such entities "are automatically considered by the U.S. government to be a 'very small business.'"[13]) Dish Network Corporation's gambit ultimately failed, but it is far from the only instance where auction participants have attempted to take advantage of the designated entity program.[14]

Such scenarios invoke the concept of "regulatory miasma." Coined by Robert Reich in a 1987 essay, "regulatory miasma" refers to a scenario where "'[e]ach maneuver [by the regulated party] generates a counter-maneuver from the regulatory bureaucracy and Congress; every feint and dodge, a more complicated prophylactic for the next encounter. The result, over

---

[10] *OPA* § 407(c).

[11] *See* "Corporate Profile," available at https://ir.dish.com/?_ga=2.148293623.1548748713.1578937096-1134201234.1555516085.

[12] *See* Steven Davidoff Solomon, "How Loopholes Turned Dish Network Into a 'Very Small Business,'" *The New York Times* (February 24, 2015), available at https://www.nytimes.com/2015/02/25/business/dealbook/how-loopholes-transformed-dish-network-into-a-very-small-business.html ("At this point you may be scratching your head. How can Dish, a company with a $34 billion market value, be a 'very small business'? … Through sleight of hand and aggressive use of partners and loopholes, Dish turned itself into that very small business, distorting reality and creating an unfair advantage.").

[13] *See* Jeff Hawn, "Should the FCC kill the Designated Entity program?," *RCR Wireless News* (September 15, 2015), available at https://www.rcrwireless.com/20150915/policy/fcc-desginated-entity-program-shelf-life-tag15.

[14] *See* Doug Brake, "Time to End the FCC's Designated Entity Program," *Innovation Files* (September 8, 2015), available at https://www.innovationfiles.org/time-to-end-the-fccs-designated-entity-program/ (noting that "[a] 2005 Congressional Budget Office report was quite critical of the program, outlining the large numbers of licenses that eventually flowed to larger companies and how the program, especially problems with the PCS C Block restricted to only DE bidding, ended up slowing deployment of spectrum and ultimately costing consumers") (citation omitted).

time, is a profusion of legislative and regulatory detail that confounds American business.'"[15] It should go without saying that these cat-and-mouse games waste limited resources and reduce overall consumer welfare.

IV. Exclusive Enforcement by the FTC Better Serves the Goals of Privacy Oversight

Federal legislation that formalizes and makes exclusive FTC online privacy enforcement authority, by contrast, would advance consumer privacy interests while avoiding the concerns set forth above. Additional resources (*e.g.*, staff and budget) and the ability to impose fines in the first instance would expand the FTC's effectiveness. And state attorneys general, working in collaboration with the FTC, could assist with enforcement.[16]

Sole FTC responsibility for online privacy enforcement promises numerous benefits. One, enforcement by a single agency at the federal level leads to a consistent body of case law that provides clear, nationwide guidance to consumers and businesses alike. Two, the FTC is able to leverage its decades of privacy-related experience to arrive at sound, informed outcomes. Three, the FTC's flexible, case-by-case approach reflects and responds dynamically to real-world marketplace developments – and does so in a way that takes into account evolving businesses models, innovative use cases, and the specific types of personal information involved. Four, personal enrichment does not factor into the FTC's decision-making process.

FTC authority to compensate injured individuals directly, meanwhile, would address the primary justification for a private right of action – the desire to make whole those who have suffered harm – without incentivizing excessive and undesirable litigation. For example, the United States Consumer Data Privacy Act of 2019 ("USCDPA"), a discussion draft circulated late last year by Senate Commerce Committee Chairman Roger Wicker (R-MS), would make available to the FTC a "Data Privacy and Security Victims Relief Fund" that the agency could use, "without fiscal year limitation, to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which civil penalties have been imposed under this Act."[17]

Consumer welfare is maximized when enforcement strikes the proper balance between protecting consumer rights and enabling the marketplace to operate efficiently. Exclusive enforcement by the FTC is a better way to reach that optimal middle ground, as the U.S. Chamber Institute for Legal Reform well explains:

---

[15] *Id*. (quoting Robert Reich, "The Miasma of Regulation" (1987)). Brake applies the concept of "regulatory miasma" to the designated entity program and concludes that "[o]ne might be hard-pressed to find a better example."

[16] *See, e.g.*, Staff Discussion Draft, United States Consumer Data Privacy Act of 2019 § 402(a), available at https://aboutblaw.com/NaZ (*USCDPA*) ("In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by the engagement of any covered entity in an act or practice that violates this Act or a regulation promulgated under this Act, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States…."); *see also id.* § 402(b)(1) ("Except where not feasible, the attorney general of a State shall notify the [FTC] in writing prior to initiating a civil action under subsection (a). Such notice shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notice, the [FTC] may intervene in such action….").

[17] *USCDPA* § 401(a)(4)(C).

> Agency enforcement is far more beneficial to consumers and the organizations that serve them than unpredictable and excessive attorney-driven private litigation…. [P]rivacy statutes that are enforced by government agencies provide a robust process through which noncompliance with protected privacy interests can be identified, remedied, and monitored while promoting consistency, fairness, and innovation.[18]

V. Conclusion

As a mechanism to enforce privacy rights, an individual private right of action falls short. The ability of plaintiffs' attorneys to pursue class actions, meanwhile, makes matters far worse. Specific injuries can be difficult to identify, connect to those responsible, and quantify. This undermines private litigation's ability to advance effectively the goals of privacy oversight. Attempts to remedy these shortcomings (*e.g.*, statutory damage provisions) distort the incentives of consumers and the lawyers who represent them, leading to excessive litigation and an overall reduction in consumer welfare. And allowing plaintiffs' attorneys to pursue class actions exacerbates the situation by increasing dramatically the potential amounts that they might recover – while at the same time decreasing the likelihood that those aggrieved will receive their fair share.

Exclusive enforcement by the FTC, on the other hand, would avoid these shortcomings. It also would protect adequately consumer privacy interests, provide clear, nationwide rules of the road to consumers and businesses alike, be responsive to marketplace developments, and provide harmed individuals with proper compensation.

* Andrew Long is a Senior Fellow of the Free State Foundation, an independent**,** nonpartisan free market-oriented think tank located in Rockville, Maryland.

[18] U.S. Chamber Institute for Legal Reform, "Ill-Suited: Private Rights of Action and Privacy Claims" (July 2019), available at https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf, at 19.