

2023

## Exploring Financial Data Protection and Civil Liberties in an Evolved Digital Age

Amanda Lindner  
*Fordham University School of Law*

Follow this and additional works at: <https://ir.lawnet.fordham.edu/jcfl>



Part of the [Banking and Finance Law Commons](#), [Consumer Protection Law Commons](#), [Finance and Financial Management Commons](#), [Privacy Law Commons](#), [Science and Technology Law Commons](#), and the [Technology and Innovation Commons](#)

---

### Recommended Citation

Amanda Lindner, Comment, Exploring Financial Data Protection and Civil Liberties in an Evolved Digital Age, 28 Fordham J. Corp. & Fin. L. 271 (2023).

This Comment is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Journal of Corporate & Financial Law by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact [tmelnick@law.fordham.edu](mailto:tmelnick@law.fordham.edu).

# EXPLORING FINANCIAL DATA PROTECTION AND CIVIL LIBERTIES IN AN EVOLVED DIGITAL AGE

*Amanda Lindner\**

## ABSTRACT

There is no comprehensive financial privacy law that can protect consumers from a company's collection sharing and selling of consumer data. The most recent federal financial privacy law, the Gramm-Leach-Bliley Act ("GLBA"), was enacted by Congress over 20 years ago. Vast technological and financial changes have occurred since 1999, and financial privacy law is due for an upgrade.

As a result, loopholes exist where companies can share financial data without being subject to laws or regulations. Additionally, federal financial privacy related laws provide little to no recourse for consumers to self-remediate with litigation, also known as a private right of action. This Comment explores the current regulations relating to consumer privacy, the protection of non-public consumer information, and the current issues associated with the consumer protection laws' lack of private a right of action. This Comment investigates the policy implications of a private right of action for consumer financial privacy and suggests how future regulation or amendments to existing law protect consumers in the digital age. Finally, it explores potential policy solutions and posits that there can be a private right of action middle-ground.

INTRODUCTION .....	272
I. BACKGROUND .....	274
A. Protection of Consumer Financial Information is Imperative to Civil Liberties .....	274
B. Disclosure is Not a Comprehensive Mechanism of Justice .....	276
C. Current Consumer Financial Privacy Framework .....	276

---

\* J.D., Fordham University School of Law, 2022; B.S. Cornell University, 2015. Thank you to the *Fordham Journal of Corporate & Financial Law* for its outstanding edits and continued contributions, both as a writer and an editor. I also thank Matthew and Andrea for unyielding love and support—you are my light.

D. Comparative Regulation Regimes .....	278
<b>II. ISSUE: PRIVACY HARMS MERIT A PRIVATE RIGHT OF ACTION BUT FACE UPHILL LEGAL CHALLENGES.....</b>	<b>280</b>
A. Standing Issues with the Private Right of Action.....	281
B. Privacy Litigants Face Obstacles in Proving Harm .....	282
<b>III. SOLUTIONS TO THE PRIVATE RIGHT OF ACTION CONSEQUENCES .....</b>	<b>283</b>
A. The Ability to Sue Allows Citizens to Actively Engage in Their Legal Right to Privacy.....	285
<b>IV. SOLUTION: FINDING A PRIVATE RIGHT OF ACTION MIDDLE GROUND .....</b>	<b>287</b>
<b>CONCLUSION.....</b>	<b>289</b>
<b>APPENDIX.....</b>	<b>290</b>

## INTRODUCTION

The modern technological revolution promises increased convenience, economies of scale, disruption in an existing marketplace, information transparency, and democratization of whole sectors.<sup>1</sup> At odds with this innovation are questions of how companies collect, share, and even sell consumer data in exchange for the aforementioned benefits.<sup>2</sup> Some financial technology companies (“FinTechs”) create applications that promise streamlined processes while simultaneously selling consumer data for profit.<sup>3</sup> As a result, many customers may not understand or realize their data has been shared with other parties.<sup>4</sup>

For example, in 2019, the Federal Trade Commission (“FTC”) issued an enforcement action against LightYear Dealer Technologies (“LightYear”) because it enabled dealers to hold and maintain personal financial information.<sup>5</sup> The FTC found LightYear, a software and data

---

1. See LAUREN SAUNDERS, NAT’L CONSUMER LAW CTR., FINTECH AND CONSUMER PROTECTION: A SNAPSHOT 3 (2019), <https://www.nclc.org/images/pdf/cons-protection/rpt-fintech-and-consumer-protection-a-snapshot-march2019.pdf> [<https://perma.cc/X275-QQVC>].

2. See *id.*

3. See *id.* at 9.

4. See *id.*; see also *Key Findings from the Consumer Digital Behavior Study*, KEARNEY, <https://www.kearney.com/financial-services/the-consumer-data-privacy-marketplace/the-consumer-digital-behavior-study> [<https://perma.cc/JTJ5-2TV9>] (last visited Oct. 19, 2022).

5. LightYear Dealer Techs., LLC, No. C-4687 FTC (2019),

processing company for car dealership in violation of federal privacy law because it stored and shared customers' private financial information without their consent.<sup>6</sup> The FTC reasoned LightYear was a financial institution because it is a data processing product that facilitated credit to consumers.<sup>7</sup> However, there are countless other technology companies that may not qualify as a financial institution that collect and share personal financial information.<sup>8</sup>

While there are various tools and laws proposed and enacted to help protect consumers, there is no comprehensive financial privacy law that can tackle modern day issues.<sup>9</sup> The Consumer Financial Protection Bureau ("CFPB") and the Federal Communications Commission ("FCC") share the responsibility of regulating financial privacy. The most recent federal financial privacy law, the Gramm-Leach-Bliley Act ("GLBA"),<sup>10</sup> was enacted by Congress over 20 years ago. Vast technological and financial changes have occurred since 1999, and financial privacy law is due for an upgrade.

As a result, loopholes exist where FinTechs can share financial data without being subject to laws or regulations. Additionally, most consumer protection regulation and legislation have traditionally focused on disclosure, which is not a comprehensive mechanism of justice.<sup>11</sup> Disclosure includes governmental or regulatory bodies requiring entities to showcase certain information to the public, such as, filings or warning labels. Federal financial privacy related laws provide little to no recourse for consumers to self-remediate with litigation, also known as a private right of action.<sup>12</sup> Does the law reject someone's personhood if it limits her ability to sue based on her statutory right? There is a level of autonomy and dignity that a person gains from her right to sue. Citizens should be

---

[https://www.ftc.gov/system/files/documents/cases/172\\_3051\\_c-4687\\_dealerbuilt\\_decision\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf) [<https://perma.cc/RV6N-QUSP>].

6. *See id.*

7. *See id.*

8. *See* SAUNDERS, *supra* note 1, at 9.

9. *See infra* Appendix.

10. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

11. *See* Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today—And How to Change the Game*, BROOKINGS (July 12, 2018) <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/> [<https://perma.cc/W2PY-3Y7Y>].

12. *See id.*

given the same litigative opportunities to protect their financial privacy rights as other areas of the law such as civil rights and employment rights.

This Comment explores the current regulations relating to consumer privacy and the protection of non-public consumer information. Current consumer privacy protection regulation is insufficient. It does not allow consumers to actively participate in their protection, thereby denying their civil liberties. In Part I, this Comment explores why strong consumer financial protection is important to protect civil liberties. Part I also identifies the current landscape of consumer financial privacy laws and the inability of individuals to sue based on a statute. Part II explores the legal challenges of a private right of action, including the large issue of Article III standing. Part II lays out the issues associated with the consumer protection laws' lack of private a right of action and hypothesizes that this could be a powerful solution to protect consumers. Part II also identifies other state regulations, such as the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act, that provide a private right of action. Part III explores the policy implications of a private right of action for consumer financial privacy and suggests how future regulation or amendments to existing law protect consumers in the digital age. Part IV identifies potential policy solutions and posits that there can be a private right of action middle-ground.

## I. BACKGROUND

### A. PROTECTION OF CONSUMER FINANCIAL INFORMATION IS IMPERATIVE TO CIVIL LIBERTIES

Consumer financial privacy includes the protection of non-public financial-related personal information.<sup>13</sup> For example, consumer financial information includes, but is not limited to: credit card and social security information; payday loans; medical, utility, and telephone accounts; as well as insurance, residential, and employment history.<sup>14</sup>

There are benefits to having little regulation protecting consumer financial information. For example, it allows new entrants in the market to have access to consumer data that would otherwise be unavailable.<sup>15</sup>

---

13. See Leon Yehuda Anidjar & Inbar Mizrahi-Borohovich, *Reinventing Credit Data Sharing Regulation*, 29 S. CAL. INTERDISC. L.J. 177, 182 (2019).

14. *Id.* at 178.

15. *Id.* at 181.

Similarly, access to consumer financial information could increase access to credit for those who traditionally have trouble tapping into the credit market. This is because free flow of information makes the cost of credit less expensive.<sup>16</sup> Finally, if financial information is more transparent, it creates an incentive for people to pay back loans and other bills.<sup>17</sup> If individuals are delinquent, lenders will be aware of this information and may be less inclined to lend in the future.<sup>18</sup> While open sharing of consumer financial information is valuable to institutions such as banks, insurance companies, and other lenders, it comes at a cost that likely outweighs the benefits.

FinTechs and technology companies that harbor important financial information serve as gatekeepers of valuable personal information. However, holding and disclosing this information can lead to overt discrimination by excluding certain groups from credit based on their past financial information.<sup>19</sup> This will then continue to perpetuate the cycle of economic hardship that facilitated financial delinquency.<sup>20</sup> Sharing of consumer financial information ultimately causes those who may benefit most from consumer credit, housing, insurance, and education to be ignored by the institutions collecting and utilizing financial data.<sup>21</sup>

Additionally, privacy breaches perpetuate compounded harm for marginalized groups.<sup>22</sup> This is because the information can be synthesized from various data points about each individual and stored permanently.<sup>23</sup> Consumers have little to no ability to change their classification.<sup>24</sup> The information may also be incorrect and the consumer cannot rectify the error.<sup>25</sup> This can have substantial long-term effects on their ability to access credit, work in certain vocations, or rent homes.<sup>26</sup> For these reasons, the government has recognized the importance of protecting consumer financial information in various formats.<sup>27</sup> However, there is a

---

16. *See id.* at 178.

17. *See id.* at 182.

18. *See id.*

19. *Id.* at 184.

20. *See id.*

21. *See id.*

22. *See id.*

23. *See id.* at 196.

24. *Id.* at 183.

25. *See id.* at 184.

26. *See id.* at 185.

27. *See, e.g.,* 15 U.S.C. § 78o.

significant gap in the law that Congress must address due to emerging technology and loopholes in the current regulatory framework to protect consumer financial privacy.<sup>28</sup>

#### B. DISCLOSURE IS NOT A COMPREHENSIVE MECHANISM OF JUSTICE

There are federal laws that mandate company disclosure of how financial information will be stored and used.<sup>29</sup> Often the privacy laws that enable disclosure are “obscure and complex,” making it difficult for a layperson to understand.<sup>30</sup> Similarly, there is little to no choice in accepting a product that someone may want or need because a consumer has such little bargaining power.<sup>31</sup> The need for the product could make the disclosure a contract of adhesion.<sup>32</sup>

Lawmakers can use other policy tools to supplement disclosure. While there are various other policy tools,<sup>33</sup> this Comment focuses on the private right of action. A private action occurs when a company violates an individual’s statutory privacy right; the individual can then sue the company based on the statute.<sup>34</sup> While a private right of action is highly controversial, allowing this right contributes to a person’s civil liberties and identity of personhood.<sup>35</sup>

#### C. CURRENT CONSUMER FINANCIAL PRIVACY FRAMEWORK

Without an omnibus federal privacy law, various federal laws protect the financial privacy of consumers.<sup>36</sup> Additionally, there are other arms of state governments that aim to protect consumers, and all 50 states and

---

28. See *infra* Section I.C.

29. See 15 U.S.C. § 6801; see also *infra* notes 36-42.

30. See Kerry, *supra* note 11.

31. See *id.*

32. See *id.*; see also *Berkson v. Gogo LLC*, 97 F. Supp. 3d 359, 388-89 (E.D.N.Y. 2015) (outlining a standard for considering a privacy policy an electronic contract of adhesion).

33. See *infra* Appendix.

34. See generally *State Consumer Protection Offices*, USA <https://www.usa.gov/state-consumer>.

35. See Lauren Henry Scholz, *The Significance of Private Rights of Action in Privacy Regulation*, CORNELL UNIV. (Oct. 15, 2021), [https://vod.video.cornell.edu/media/Clip+of+TLC+Fall+2021+10+15+2021+%5Blauren+Scholz%5D/1\\_wb61x8nd](https://vod.video.cornell.edu/media/Clip+of+TLC+Fall+2021+10+15+2021+%5Blauren+Scholz%5D/1_wb61x8nd) [https://perma.cc/JZD2-9AJF].

36. See *infra* notes 38-40.

territories have state consumer protection offices.<sup>37</sup> For instance, the Fair Credit Reporting Act allows for a private right of action.<sup>38</sup> Additionally, other descendants of that law, including the Right to Financial Privacy Act, Cable Communications Policy Act, and the Electronic Communications Privacy Act allow for the private right of action in numerous capacities.<sup>39</sup> While the private rights of action exist for the aforementioned statutes, the privacy statutes pertain only to narrow rights such as credit reporting and television usage.<sup>40</sup> Unfortunately, it is not broad enough to encompass modern financial privacy law.<sup>41</sup>

More relevant for modern financial privacy law, Congress enacted the GLBA in 1999 to ensure that companies: (1) do not share consumers' financial data without consumer consent; and (2) enable proper methods to prevent data breaches.<sup>42</sup> Notably, the GLBA requires financial institutions to disclose their information-sharing processes and appropriately protect consumer non-public information.<sup>43</sup> The CFPB and FTC jointly enforce consumer-related privacy provisions of the GLBA.<sup>44</sup>

---

37. See generally *State Consumer Protection Offices*, USA <https://www.usa.gov/state-consumer>.

38. See Cameron F. Kerry & John B. Morris, Jr., *In Privacy Legislation, a Private Right of Action Is Not an All-or-Nothing Proposition*, BROOKINGS: TECHTANK (July 7, 2020), <https://www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/> [<https://perma.cc/2CQ5-NLLU>].

39. See *id.*

40. See *id.*

41. See *id.* Additionally, Congress passed the Consumer Credit Protection Act to regulate the consumer credit industry and protect consumers from unfair commercial practices. See 15 U.S.C. § 1601. However, as practices in the financial industry evolved, consumers required even more regulation to combat unaddressed issues. *But see Consumer Credit*, CORNELL LEGAL INFO. INST., [https://www.law.cornell.edu/wex/consumer\\_credit](https://www.law.cornell.edu/wex/consumer_credit) [<https://perma.cc/Z4T4-4QPV>].

42. See 15 U.S.C. § 6801; see also FTC, Gramm-Leach-Bliley Act, FTC.gov, <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act> [<https://perma.cc/Y9JX-9D74>].

43. See 15 U.S.C. § 6801.

44. Fara Soubouti, *Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection*, 24 N.C. BANKING INST. 527, 528 (2020). The FTC tackles the Privacy of Consumer Financial Information Rule, applying to non-bank financial institutions. The “Privacy Rule” and the CFPB enforce the Privacy of Consumer Financial Information Regulation, which applies to financial institutions (“Regulation P”). *Id.*; see also 15 U.S.C. § 6805(a).



There are many blind spots in the GLBA. The GLBA applies to “any financial institution that provides financial products or services to consumers.”<sup>45</sup> Many other entities who collect, store, and utilize customers’ non-public information do not have to comply with the GLBA requirements, even though it may have the same financial information as financial institutions.<sup>46</sup> Additionally, because Congress created the GLBA in 1999, way before some technologies were a twinkle in an engineer’s eye, the GLBA does not allow for a private right of action.<sup>47</sup>

#### D. COMPARATIVE REGULATION REGIMES

Discussed in the last section, there is relatively little ability for individuals to sue to protect their data privacy in the United States.<sup>48</sup> However, some states enable a private right of action,<sup>49</sup> which serves as a helpful comparison point as policymakers build other privacy laws.

In passing the Illinois Biometric Information Privacy Act (“BIPA”), the Illinois legislature enabled a person to recover up to \$5,000 per incident from a violator.<sup>50</sup> Additionally, the Illinois State Supreme Court recently held in *Rosenbach v. Six Flags Entertainment Corp.*<sup>51</sup> that individuals may sue under BIPA even if they do not have any actual harm or damage, so long as there was a technical violation of the law.<sup>52</sup> The court noted that Illinois case law interpreted statutes with similar verbiage such as the AIDS Confidentiality Act and found no requirement for a plaintiff to prove actual harm.<sup>53</sup> This is significant because compared to

---

45. A company is a financial institution if it engages in activities “financial in nature or incidental to a financial activity.” FED. RESERVE, FREQUENTLY ASKED QUESTIONS FOR THE PRIVACY REGULATION 1 (Dec. 2001), <https://www.federalreserve.gov/boarddocs/press/general/2001/200112122/attachment.pdf> [https://perma.cc/VE84-CTGB]. Examples of activities financial in nature include lending, investing, safeguarding money, insuring, or providing financial advice, and market making. 15 U.S.C. § 6809.

46. See 15 U.S.C. § 6801-6809.

47. See 11 U.S.C. § 6805(a).

48. Indeed, only a few states currently have a private right of action for privacy-related breaches. See *supra* Section I.C.

49. See *id.*

50. 740 ILL. COMP. STAT. 14/1 (2008).

51. 129 N.E.3d 1197 (Ill. 2019).

52. See *id.* at 1204. In *Rosenbach*, an amusement park fingerprinted a minor without parental consent, thus violating the BIPA. *Id.* at 1200.

53. *Id.* at 1204.

Article III standing case law,<sup>54</sup> the *Rosenbach* court significantly reduced barriers for plaintiffs to overcome a motion to dismiss and recover.<sup>55</sup>

*Rosenbach* kicks the door wide open to enable litigation targeted towards FinTech.<sup>56</sup> As a result, scholars foresee that FinTech will have added legal, compliance, and audit costs.<sup>57</sup> Within the sphere of data privacy, *Rosenbach* and BIPA provide an informative and unique comparison point to consumer financial privacy.

Enacted in 2018, the California Consumer Privacy Act (“CCPA”) “gives consumers more control over the personal information that businesses collect about them.”<sup>58</sup> The CCPA permits California-based consumers to bring civil suits for damages between \$100 and \$750 per consumer per incident so long as the information stolen from the consumer includes her first and last name in combination with other important financial information.<sup>59</sup> The CCPA provides for statutory damages,<sup>60</sup> which overcomes the strong presumption of standing.<sup>61</sup>

While this is a vast improvement from having no private right of action at all, there is a high barrier for an individual to sue a company violating CCPA; there are also exceptions violators can rely upon to reduce the chance of litigation.<sup>62</sup> For example, a victim must give a

---

54. See Soubouti, *supra* note 44, at 548; 15 U.S.C. § 6801.

55. *Rosenbach*, 129 N.E.3d at 1206.

56. See Tae Kim, *Rosenbach v. Six Flags: Illinois Supreme Court Interprets Illinois Biometric Privacy Law*, HARV. J.L. & TECH.: JOLT DIGEST (Feb. 18, 2019), <https://jolt.law.harvard.edu/digest/279rosenbach-v-six-flags-illinois-supreme-court-interprets-illinois-biometric-privacy-law> [<https://perma.cc/X95X-AJVL>].

57. *Id.*

58. CAL. CIV. CODE § 1798.150(a)(1) (West 2022); see also *California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP’T OF JUSTICE <https://oag.ca.gov/privacy/ccpa> [<https://perma.cc/G9DV-SQPS>] (last visited Oct. 19, 2022).

59. CIV. § 1798.150(a)(1)(A). The CCPA outlines some of the following as important financial information enabling someone to bring a private right of action: social security number, driver’s license number, tax identification, passport number, fingerprint, retina or iris image, or other unique biometric data, credit or debit card number if combined with any required code, or password that would allow someone to access to that account. CIV. § 1798.81.5(d)(1)(A)(i-vii).

60. CIV. § 1798.150(a)(1).

61. Jonathan Schenker, Michael F. Buchanan & Alejandro H. Cruz, *A Closer Look at the CCPA’s Private Right of Action and Statutory Damages*, PATTERSON BELKNAP: DATA SEC. L. BLOG (Aug. 22, 2019), <https://www.pbwt.com/data-security-law-blog/a-closer-look-at-the-ccpas-private-right-of-action-and-statutory-damages> [<https://perma.cc/CJ2Z-3US8>].

62. CIV. § 1798.150(b).

business 30 days' notice to cure any violation of the CCPA.<sup>63</sup> So long as the business fixes the issue and provides notice that no violations will occur in the future, an individual cannot pursue the violating business under the CCPA.<sup>64</sup>

The BIPA and CCPA allow for a private right of action within their privacy statutes; however, BIPA and CCPA are on different ends of the spectrum. Courts have broadly interpreted BIPA to allow any plaintiff to sue if an entity violated the law.<sup>65</sup> Alternatively, CCPA created exceptions to the private right to action that make it challenging for a consumer to bring a case, limiting the right to victims of only the most egregious breaches.<sup>66</sup>

## II. ISSUE: PRIVACY HARMS MERIT A PRIVATE RIGHT OF ACTION BUT FACE UPHILL LEGAL CHALLENGES

There is no way for a consumer to enforce the GLBA through litigation and ensure that companies are not misusing her information.<sup>67</sup> Instead, a consumer must “rely on the limited resources of the FTC and state attorneys general to keep companies honest.”<sup>68</sup> Generally, courts have ruled that there is no private right of action for the breach of non-public financial data.<sup>69</sup> Additionally, there is an interrelated obstacle for a plaintiff to obtain standing in privacy matters.<sup>70</sup>

---

63. *Id.*

64. *Id.*

65. *See* *Rosenbach v. Six Flags Entertainment Corp.*, 129 N.E.3d 1197, 1204 (Ill. 2019).

66. CIV. § 1798.150(b).

67. Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 351 (2013).

68. *Id.*

69. *See In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1338-42 (N.D. Ga. 2019). Plaintiffs argued the consumer reports were crucial to the financial system because of the main role reports play in the extension of credit. *Id.* at 1309. However, the court held that financial information stolen would not bear a great deal on the credit worthiness of the consumer. *Id.* at 1313.

70. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018).

A. STANDING ISSUES WITH THE PRIVATE RIGHT OF ACTION

Even if there were broader avenues for consumers to utilize financial privacy-related laws such as the GLBA, there is a difficult burden to prove standing in many data and privacy-related matters. Article III standing is the idea that in federal court, a person seeking relief must have a “personal stake in the outcome of the controversy.”<sup>71</sup> In 2013, the Supreme Court held in *Clapper v. Amnesty International USA*<sup>72</sup> that anxiety from surveillance was too nebulous to allow Article III standing.<sup>73</sup> Subsequently, the Supreme Court doubled down on the standing requirement in *Spokeo v. Robins* which held that to satisfy Article III constitutional standing, a plaintiff must show that they suffered an injury that was “actual or imminent, not conjectural or hypothetical.”<sup>74</sup> Therefore, merely arguing that someone’s data was stolen was not sufficient to show that harm is particularized and concrete.<sup>75</sup>

Most recently, the Supreme Court in *TransUnion LLC v. Ramirez* held that even if there is an express private right of action outlined in a law, the plaintiffs need to prove they suffered from particularized and individual harm.<sup>76</sup> The Court reasoned that because no harm materialized from TransUnion’s data breach, the data breach alone was insufficient for a damages claim.<sup>77</sup> Additionally, the Court noted that the harms enumerated by the plaintiffs could potentially be sufficient for Article III standing if the plaintiffs asked for injunctive relief.<sup>78</sup> If Congress passed a federal privacy law, many have questioned if a private person’s harm would pass muster when challenged using *TransUnion* as precedent.<sup>79</sup>

---

71. See *Baker v. Carr*, 369 U.S. 186, 204 (1962).

72. 133 S. Ct 1138 (2013).

73. See generally *id.*

74. *Id.* at 1548.

75. See generally *id.*

76. 594 U.S. 2190, 2221-23 (2021). In *Transunion*, the company generated creditor reports that wrongfully flagged individuals as drug traffickers and terrorists. *Id.* As a result of this inaccuracy, the flagged individuals sued TransUnion based on the Fair Credit Reporting Act. *Id.* at 2226.

77. *Id.* at 2200.

78. *Id.* at 2210.

79. See Christine S. Wilson, Fed. Trade Comm’n Comm’r, Keynote Remarks at the Duke University Sanford School of Public Policy Robert R. Wilson Distinguished Lecture Series: Exploring Options Overcoming Barriers to Comprehensive Federal Privacy Legislation (Sept. 21, 2021), <https://www.ftc.gov/system/files/documents>

Since state law does not require Article III standing, states have a better chance at creating broader, workable requirements. However, it can still vary widely from state to state. For example, in *Wells Fargo Bank, N.A. v. Jenkins*, the Georgia Supreme Court held that a bank customer could not rely upon that statutory statement of policy to create a private right of action under Georgia tort law for an alleged breach of a duty to maintain personal information as confidential.<sup>80</sup> However, since states have varying private right of action protection, some states will give more leeway to enable a consumer to sue.

#### B. PRIVACY LITIGANTS FACE OBSTACLES IN PROVING HARM

It may be difficult for a consumer to know how and when they will be harmed after a security breach occurs with their personal financial information.<sup>81</sup> Data harms are “intangible, risk-oriented, and diffuse.”<sup>82</sup> However, that does not mean consumers will not be harmed or are not entitled to recovery for the failings of the institution entrusted to safeguard important financial information.<sup>83</sup>

Professor Ryan Calo cogently identifies that privacy harms stem from the unanticipated disclosure and use of someone’s personal information.<sup>84</sup> The former induces apprehension and embarrassment from the use of sensitive personal information.<sup>85</sup> The latter justifies “an adverse action against a person” such as “when the government leverage[s] data mining of sensitive personal information to block a citizen from air travel” or when a thief commits identity theft.<sup>86</sup>

Additionally, Professors Solove and Citron argue that courts are often far too dismissive of the myriad harms associated with data-breaches and theorize that there are indeed ways that courts can assess risk and anxiety in a particularized and concrete manner to merit

---

[/public\\_statements/1596632/wilsonspeechovercomingbarriersprivacy.pdf](https://public_statements/1596632/wilsonspeechovercomingbarriersprivacy.pdf)  
[<https://perma.cc/VCB6-8SR9>].

80. See generally 744 S.E.2d 686 (Ga. 2013).

81. See Solove & Citron, *supra* note 70, at 737.

82. *Id.*

83. See *id.*

84. M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1148-49 (2011).

85. See *id.* at 1133.

86. See *id.* at 1143.

standing.<sup>87</sup> While inconsistent with the traditional legal view of harm, it is imperative for the judiciary to acknowledge the injustice of those befallen to privacy breaches.

Adding a private right of action into a federal law that protects consumers' data privacy would be a first step toward vindicating and enabling victims to seek justice. Without the courts allowing a broader standard of harm under privacy violations, the private right of action as well as general litigation becomes futile.<sup>88</sup> In *Spokeo*, the Court "recognized that 'Congress is well positioned to identify intangible harms that meet minimum Article III requirements.'"<sup>89</sup> In acknowledging this, the Court noted that Congress could create a defined privacy law that encompasses some forms of intangible harm to enable redress.<sup>90</sup> Legislators must outline and craft otherwise nebulous specific privacy harms so that it meets federal standing requirements.

### III. SOLUTIONS TO THE PRIVATE RIGHT OF ACTION CONSEQUENCES

Enabling a federal private right of action for privacy is a nuanced policy conundrum. While there are significant consequences associated with Article III standing, because the nature of technology goes beyond state lines, this is broadly a national issue. Prohibiting an individual the right to sue denies one of her civil liberties; that right should be included in a forthcoming federal privacy law.

The private right of action is so contentious that many states have failed to adopt privacy legislation for the sole reason that the bill included a private right of action provision.<sup>91</sup> For example, the Washington state legislature failed to pass a proposed privacy bill three times because legislators could not agree on the issue of a private right of action.<sup>92</sup> Indeed, there is a risk that adding the private right of action will "poison" a future privacy bill.<sup>93</sup> On the other hand, if an omnibus federal bill can

---

87. See Solove & Citron, *supra* note 70, at 737-38.

88. See *id.* at 786-87.

89. See Kerry & Morris, *supra* note 38 (quoting *Spokeo v. Robins*, 136 S. Ct. 1540, 1543 (2016)).

90. *Id.*

91. See Scholz, *supra* note 35.

92. See Aaron Nicodemus, *Private Right of Action Proving Problematic for State Privacy Laws*, COMPLIANCE WEEK (May 5, 2021, 3:40 PM).

93. See Andreas Kaltsounis, *Private Right of Action May Again Poison Washington Privacy Act*, BAKER HOSTETLER: DATA COUNSEL (Mar. 30, 2021), <https://www.baker>

be passed, it will nullify much of the difficulty some state legislatures face when trying to pass state law with a private right of action.

Businesses can see the private right of action as “an opportunistic gotcha game.”<sup>94</sup> While companies are not necessarily against all private rights of action, there is concern with “nuisance lawsuits.”<sup>95</sup> These lawsuits enable the “for-profit model of law enforcement” where private lawyers who have little accountability to the public will file cases with non-meritorious claims.<sup>96</sup> Finally, a private right of action could reduce innovation by companies, particularly in the technology space, for fear of litigation.<sup>97</sup>

While litigation is expensive, there are public benefits to discovery.<sup>98</sup> This is because discovery sheds light on things that go on behind the closed doors of companies that the public would otherwise not be able to see.<sup>99</sup> Additionally, there is a high standard for pleading in federal court, and if claims are found meritless, they will be dismissed in court at the outset.<sup>100</sup>

Since data protection filters through almost every part of the United States economy, creating a broad private right of action can increase liability for a vast number of sectors.<sup>101</sup> This would temporarily increase instability in the law as case law moves forward.<sup>102</sup> On the other hand, some scholars have argued that increased litigation is a social good because “[i]t allows participants to act out democratic ideas that are highly valued in our society.”<sup>103</sup> Since there is a current gap in consumer privacy

---

[datacounsel.com/privacy/private-right-of-action-may-again-poison-washington-privacy-act/](https://www.datacounsel.com/privacy/private-right-of-action-may-again-poison-washington-privacy-act/) [https://perma.cc/7P4Y-K3GZ].

94. See Nicodemus, *supra* note 92.

95. See Kerry & Morris, *supra* note 38.

96. See Dan M. Clark, *Private Right to Sue Under NY Data Privacy Bill Could Clog Courts, Business Leaders Say*, N.Y.L.J. (Nov. 22, 2019, 5:39 PM).

97. Jennifer Huddleston, *A Primer on Data Privacy Enforcement Options*, AM. ACTION F. (May 4, 2020), <https://www.americanactionforum.org/insight/a-primer-on-data-privacy-enforcement-options/> [https://perma.cc/4GXR-KMN4].

98. See Scholz, *supra* note 35.

99. See *id.*

100. See Fed. R. Civ. P. 12(b)(6); see also *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

101. See Clark, *supra* note 96.

102. See Huddleston, *supra* note 97.

103. See Alexandra Lahav, *In Praise of Litigation*, DAILY J. (Nov. 8, 2017), <https://www.dailyjournal.com/articles/344760-in-praise-of-litigation> [https://perma.cc/W22X-D5AC].



case law, increased litigation would help fill out the hollowed law.<sup>104</sup> The process of allowing for cases to make their way through courts is “part of a broader flexible and risk-based approach to protecting privacy” because it enables the law to play out in accordance with society’s values.<sup>105</sup>

Additionally, it will be difficult for marginalized groups most affected by privacy-related issues to litigate because they likely do not have the resources to deploy representation to fight the breaching companies in court. On the other hand, individuals can join a class action lawsuit to reduce costs among plaintiffs who otherwise would not have the resources to sue.<sup>106</sup>

A. THE ABILITY TO SUE ALLOWS CITIZENS TO ACTIVELY ENGAGE IN THEIR LEGAL RIGHT TO PRIVACY

One of the larger relevant sociological questions here is: does the law reject someone’s personhood if it limits her ability to sue based on her statutory right? This moral question is answered in the affirmative because a person gains autonomy and dignity from her right to sue.<sup>107</sup> Giving only the government the right to sue embeds paternalism into the legal framework.<sup>108</sup> In other words, the legislature does not believe that the public can be trusted to use its litigative power effectively. Depriving the public of the power to sue is a grave error.

The instrumental aspect of the private right of action is something that the government cannot reproduce on behalf, or instead, of consumers due to the government’s resource constraints.<sup>109</sup> The government operates on a zero-sum game where there may simply be more “important” issues facing the FTC and CFPB than the collecting, sharing, and selling of consumer financial information.<sup>110</sup>

Enforcement actions within the government cannot adequately protect the financial privacy rights of consumers because these rights are

---

104. *Id.*

105. *See* Kerry & Morris, *supra* note 38.

106. *See* Stephanie A. Kuhlmann, *Do Not Track Me Online: The Logistical Struggles over the Right “To Be Let Alone” Online*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 229, 268 (2011).

107. *See* Scholz, *supra* note 35.

108. *See id.*

109. *See id.*

110. *See id.*



susceptible to regime changes that may differ based on who is in power.<sup>111</sup> There may be a desire for one regime to avoid the administrative and enforcement burden of taking up a matter.<sup>112</sup> This is because if there is pushback regarding controversial enforcement actions from important stakeholders,<sup>113</sup> regulators will be blamed along with related political regimes. Allowing individuals to sue will remove the politicization and pressure of interest groups from the basic need to protect consumer financial privacy rights.<sup>114</sup>

Additionally, because of the limited resources the government has, it may not be able to fully understand what is going on behind the closed doors of corporations as quickly as private actors. Conversely, private actors will be better up to speed on nuanced technological challenges and exploitations that companies may utilize to obtain and sell consumer financial information. For example, it took the FTC over 4 years to respond and punish LightYear.<sup>115</sup> If consumers had the ability to get involved, it is possible that the challenge for LightYear's information breach practices could have come earlier.

Instead, if there is a hybrid model of enforcement among private citizens and the government, there will likely be greater compliance with the law, along with a reduction in politicizing the issue of consumer financial privacy. A private right of action enables consumers to not only seek redress for harms, but also acts as "force multipliers to the Federal Trade Commission and state attorneys general."<sup>116</sup> The hybrid model enhances enforcement of financial privacy.<sup>117</sup>

A stronger federal data protection framework will help to provide benefits not only to consumers and large corporations, but also to small businesses.<sup>118</sup> For example, it is often challenging for small businesses to

---

111. *Id.*

112. See James J. Park, *Rules, Principles, and the Competition to Enforce the Securities Laws*, 100 CAL. L. REV. 115, 176 (2012).

113. See *id.*

114. See *id.*

115. Decision and Order, LightYear Dealer Techs., LLC, FTC Docket No. C-4687 (Sept. 3, 2019), [https://www.ftc.gov/system/files/documents/cases/172\\_3051\\_c-4687\\_dealerbuilt\\_decision\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf) [<https://perma.cc/3KWH-RXSY>].

116. See Kerry & Morris, *supra* note 38.

117. *Id.*

118. Nadia Udeshi, *Saving Small Business from the Big Impact of Data Breach: A Tiered Federal Approach to Data Protection Law*, 14 BROOK. J. CORP. FIN. & COMM. L. 389, 411 (2020).

comply with various state laws that may have different rules, levels of enforcement, and penalties.<sup>119</sup> Instead, an omnibus federal bill that ensures data protection for consumers would be less costly and easier to follow for enterprises with limited resources for legal and compliance.<sup>120</sup>

By implementing a private right of action, it can allow companies to take regulation seriously and flow internal funding towards privacy protection.<sup>121</sup> For example, knowing that the law invites consumers to sue companies will incentivize the companies to increase compliance departments so that they follow the law. Otherwise, the chances that consumers sue will increase because unlike the government's zero sum game, countless private actors, either as an individual or in a class action lawsuit, can hire private counsel and litigate if a company violates their rights.

Finally, citizens should be given the same legal rights to protect their financial privacy as their ability to protect civil rights and employment rights.<sup>122</sup> Courts have upheld the private right of action because they interpreted relevant law to include civil rights and employment rights.<sup>123</sup> Financial privacy issues create similar concerns to civil and employment matters.

An increase in litigation will continue the iterative process of defining a person's privacy rights. The goal is that case law will move forward in a direction that will be fair to both companies and consumers. The best way forward is to allow a hybrid enforcement model where individuals and the government have the statutory right to sue.

#### **IV. SOLUTION: FINDING A PRIVATE RIGHT OF ACTION MIDDLE GROUND**

A private right of action does not have to be a binary policy choice.<sup>124</sup> While the CCPA and BIPA represent opposite sides of the private right of action spectrum, it is possible to find a middle ground where those

---

119. *Id.* at 398.

120. *Id.* at 413.

121. *See* Asay, *supra* note 67, at 351.

122. *See, e.g.*, TITLE IX LEGAL MANUAL, U.S. DEP'T. OF JUST. § VIII.

123. *Id.*

124. *See* Joseph Jerome, *Private Right of Action Shouldn't Be a Yes-No Proposition in Federal U.S. Privacy Legislation*, IAPP (Oct. 3, 2019), <https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/> [<https://perma.cc/8XUY-DFDN>].

harmed may find redress, as well as preventing non-meritorious lawsuits as much as possible.<sup>125</sup> There are many creative solutions that enable individuals to sue, some of which are listed here; however, this is only a sampling of the many robust options policymakers can choose.

For instance, Cameron F. Kerry and John B. Morris, Jr. recommend allowing a private right of action in “cases of ‘willful or repeated’ violations.”<sup>126</sup> Kerry and Morris argue that this “willful and repeated” standard can prevent nuisance lawsuits because only companies with harmful patterns and practices will be targets for the private right of action.<sup>127</sup> In practice, federal law enforcement agents would determine if the entities willfully and repeatedly violated the law in accordance with internal policy standards or case law. Similar to the CCPA, where a plaintiff must give a company 30 days to cure before she can sue for statutory damages.<sup>128</sup> Kerry and Morris articulate that one-time events would be excluded from the statutory private right of action to reduce nuisance lawsuits, even though they affect many individuals.<sup>129</sup>

Additionally, others have advocated for the availability of injunctive relief to stop privacy-related harms.<sup>130</sup> Injunctive relief refers to a court order that prevents an entity from doing something that has been shown to be irreparably damaging. In order for a person to successfully enjoin an entity from continuing their data practices, a person would have to show in federal court that: (1) they would suffer irreparable injury without an order; and (2) the moving party has a substantial likelihood of success on the merits.<sup>131</sup> After receiving the injunction, the entity that has been using financial information without a consumer’s consent would stop.<sup>132</sup> The limitations of this would include that the injunctive relief may not account for the actual harm that a consumer has faced, and therefore will not properly right the wrong of the violating entity. Similarly, the bar for getting an injunction is quite high, as the damage must be considered irreparable to the moving party. As a result, the harm may be great, but not considered irreparable under the interpretation of the judge. On the other hand, allowing consumers to sue for injunctive relief if defendants

---

125. *Id.*

126. *See* Kerry & Morris, *supra* note 38, at 6.

127. *Id.*

128. CAL. CIV. CODE § 1798.150(b) (West 2022).

129. *See* Kerry & Morris, *supra* note 38, at 6.

130. Huddleston, *supra* note 97.

131. *See* 28 U.S.C. § 122a.

132. *Id.*

have allegedly infringed on their privacy rights serves as a middle ground because it takes away the monetary incentive that mass tort litigation propagates.<sup>133</sup>

If politicians are afraid of the monetary incentive to litigation, a federal privacy law can include a damages cap.<sup>134</sup>

Since consumer privacy is an area of the law with thin case law, Congress can create sunset provisions<sup>135</sup> to build precedent for the private right of action to occur so that mass tort litigation does not continue after a certain timeframe.<sup>136</sup> Sunset legislation promises a means for legislators to reassess if the policy is working as policymakers intended.<sup>137</sup> However, this assumes that the policymakers can get the consensus required to re-install provisions in the statute, if needed. Sunset legislation can encourage stability in the law over time by cementing case law concerning private litigants after a certain point.

Privacy is “about being able to participate in society and knowing your data isn’t going to be abused.”<sup>138</sup> While giving individuals the tools to fight back may have costs, the benefits outweigh those costs. Legislators should come up with creative solutions so that passing privacy bills will not be an impossible feat if the legislation incorporates some form of private rights of action.

## CONCLUSION

While there are tools that regulators and consumers can use to provide greater privacy rights, current federal regulation is insufficient to adequately protect individuals from privacy harms. One method is enabling consumers to sue to address and rectify privacy abuse by companies. Challenges of a federal private right of action in a privacy law include standing. While the private right of action in privacy matters is imperfect, if properly narrow it provides one method to enable justice and

---

133. Huddleston, *supra* note 97.

134. See Scholz, *supra* note 35.

135. A sunset provision is a specific provision or entire law that expires after a certain point in time. See Rebecca M. Kysar, *The Sun Also Rises: The Political Economy of Sunset Provisions in the Tax Code*, 40 GA. L. REV. 335, 337 (2006).

136. See Scholz, *supra* note 35.

137. See Kysar, *supra* note 135, at 338.

138. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the U.S. (and Why It Matters)*, N.Y. TIMES (Sept. 6, 2021) <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/> [<https://perma.cc/DGV4-LTEW>].

protect consumers. Finally, giving individuals a private right of action empowers consumers to take matters into their own hands. Allowing a consumer the right to choose if she would like to pursue violators of the law against her is a civil liberty and each consumer should have the right to protect herself as technology evolves.

#### APPENDIX

The following include other alternatives to increase enforcement of financial consumer privacy law other than the private right of action:

**1. Increased budget for the FTC/CFPB.** Regulators are “constantly outgunned by powerful business groups.”<sup>139</sup> To give regulators ammunition, the government can increase budget allocation to further regulatory programs.<sup>140</sup> However, regulatory agencies faced backlash from Congress and the public in the past for being too aggressive.<sup>141</sup> Additionally, many may be hesitant to continue expansion of the federal government.

**2. Self-Governance.** The CFPB and FTC are simply unable to monitor all privacy-related activities of private companies.<sup>142</sup> As a result, regulators advocate and require self-regulation in the form of compliance departments.<sup>143</sup> The government will work with the company to plan the

---

139. Chris Jay Hoofnagle et al., *The FTC Can Rise To the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS: TECHTANK (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/> [<https://perma.cc/KE45-NUYX>].

140. *See id.* The FTC currently has around 50 staff members dedicated to privacy matters. Conversely, the United Kingdom’s Information Commissioner’s Office employs 700 focused on privacy and data protection. *Id.*

141. *See* Chris Hoofnagle, *KidVid in Context*, TECHNOLOGY ACADEMICS POLICY, (June 8, 2018), <https://www.techpolicy.com/Blog/Featured-Blog-Post/%E2%80%8BKidVid-in-Context.aspx> [<https://perma.cc/5KN9-9XVC>]. In the 1970s, the FTC attempted to regulate advertising focused on children which enraged Congress and impelled Congress to shut the FTC down temporarily. *Id.*

142. Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 COLUM. L. REV. 369, 398 (2019).

143. *Id.* at 398-99. For example, Goldman Sachs, among other large financial institutions, increased its compliance division threefold to around 950 individuals from 2004 to 2016. Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467, 510 (2020). Conversely, the CFPB has a workforce of around 400 to conduct examinations of large global banks including Goldman and Citi Bank. *Id.*

internal management and then will engage in a “top-down assessment” of a firm’s self-monitoring.<sup>144</sup>

**3. Third party intermediaries.** As opposed to internal executors of law, regulation or internal policies, policymakers can enable consumer privacy enforcement through regulation of large “gatekeeping” companies such as Facebook, Amazon, Google, and Apple (“Big Tech”) that have platforms for other companies to sell and market products.<sup>145</sup>

---

144. Van Loo, *supra* note 142, at 399. Top-down assessments often come in the form of risk assessment where compliance members and auditors will present requested information to regulators. *Id.*

145. *Id.* at 482-84.