Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection

Fara Soubouti

Follow this and additional works at: https://scholarship.law.unc.edu/ncbi

Part of the Banking and Finance Law Commons

Recommended Citation
Available at: https://scholarship.law.unc.edu/ncbi/vol24/iss1/23
Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection

I. INTRODUCTION

Industry leaders are no longer asking if a comprehensive federal data privacy law should be implemented; instead the question has shifted to how it should be implemented.\(^1\) In response to a growing number of data breaches\(^2\) and the European Union’s General Data Protection Regulation\(^3\) (“GDPR”), states are adopting their own data privacy legislation. These state changes have led to a patchwork of state laws that U.S. companies are struggling to satisfy.\(^4\) To unify the patchwork of data privacy laws across the U.S., lawmakers have introduced numerous federal privacy proposals over the past year.\(^5\) Committees in both the House and Senate have sought feedback from stakeholders to evaluate

---


5. See Lazzarotti, supra note 4 (discussing data privacy legislative proposals at the state level).
legislative solutions, while the Federal Trade Commission (“FTC”) has held hearings to help shape the legislative debate.

Although banks are currently subject to the privacy provisions of the Gramm-Leach-Bliley Act of 1999 (“GLBA”), banks often gather consumer information that is not protected by the GLBA; this is the type of consumer data that should be protected by a comprehensive federal privacy law. Such comprehensive federal privacy legislation should preempt state privacy laws to avoid inefficiencies associated with the industry’s compliance with a patchwork of state laws. However, a federal data privacy law that preempts state laws should have strong data protections to maintain consumer trust. While the GLBA has helped

---


12. See Developing the Administration’s Approach to Consumer Privacy, Notice of Request for Public Comments, 83 Fed. Reg. 187, 48600 (proposed Sept. 26, 2018) (“Trust is at the core of the United States’ privacy policy formation.”). Public concern of privacy and security on the Internet could hinder the growth of the digital economy. NAT’L TELECOMM. & INFO. ADMIN., Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds, NAT’L TELECOMM. & INFO. ADMIN.: BLOG (Aug. 20, 2018), https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds [https://perma.cc/UD7J-QGYC] (“[P]rivacy concerns may lead to lower levels of economic productivity as people decline to make financial transactions on the Internet. . . . [A]t least a third of online households have been deterred from certain forms of online activity, such as financial transactions, due to privacy and security concerns.”).
consumers trust banks with their data,\textsuperscript{13} it is unclear how long consumers will trust financial institutions if consumers continue to fall victim to data breaches and lose confidence in banks’ information sharing practices.\textsuperscript{14}

This Note proceeds in six parts. Part II discusses the case for preemption of the current patchwork of state data privacy laws and the role of the GLBA in a federal privacy framework.\textsuperscript{15} Part III analyzes the scope of federal privacy legislation through the definition of personal data and its effect on financial institutions.\textsuperscript{16} Part IV explores the user control rights that federal privacy law should require banks to provide consumers.\textsuperscript{17} Part V evaluates how a comprehensive federal data privacy law can impose external accountability on financial institutions through various enforcement efforts.\textsuperscript{18} Part VI concludes this Note.\textsuperscript{19}

II. PREEMPTION OF STATE DATA PRIVACY LAWS AND AMENDING THE GLBA

Preemption is a divisive and high-stakes issue because it impacts all aspects of existing and future privacy law.\textsuperscript{20} There are two ways to

---


\textsuperscript{14} The U.S. Department of Commerce’s National Telecommunications and Information Administration (“NTIA”) conducted a national survey in 2017 that found consumer concerns related to Internet transactions included “identity theft, credit card or banking fraud, data collection by online services, loss of control over personal information, data collection by government, and threats to personal safety.” NAT’L TELECOMM. & INFO. ADMIN, supra note 12.

\textsuperscript{15} While data breach notification is an important issue in the data privacy and security debate, this Note does not address data breach requirements in the context of future federal data privacy law. Id.

\textsuperscript{16} See infra Part II.

\textsuperscript{17} See infra Part III.

\textsuperscript{18} See infra Part IV.

\textsuperscript{19} See infra Part V.

approach federal preemption of existing privacy laws.\textsuperscript{21} A federal data privacy law can preempt state data privacy laws by establishing a ceiling\textsuperscript{22} or serving as a federal baseline that allows for stricter state laws.\textsuperscript{23} For example, the GLBA has an anti-preemption provision that sets a federal statutory floor, allowing states to pass more stringent state laws.\textsuperscript{24} Additionally, a federal data privacy law can affect existing federal sectoral data privacy laws, such as the GLBA, by exempting entities covered by existing sectoral laws from compliance with the new federal law.\textsuperscript{25} Conversely, a new federal law could require covered entities to comply with the new federal law in addition to the existing sectoral privacy law, and where the laws conflict, the covered entities would have to follow the stricter law.\textsuperscript{26} Since stakeholders seek uniformity in their privacy compliance efforts, lawmakers should resolve the question of preemption of state laws and conflicting federal laws so that stakeholders effectively understand their privacy obligations.\textsuperscript{27}

\textbf{A. Preemption of State Data Privacy Laws}

The concept of preemption has often baffled legislators because it is a “more intricate and highly contested provision” of lawmakers’ legislative proposals.\textsuperscript{28} Consequently, few legislative proposals for a comprehensive federal privacy law include provisions that preempt state

\begin{itemize}
\item \textsuperscript{21} See Paul M. Schwartz, Preemption \& Privacy, 118 Yale L.J. 902, 946 (2009) (explaining the possible approaches to federal preemption in context of privacy law).
\item \textsuperscript{22} The National Labor Relations Act (“NLRA”) establishes a federal ceiling that preempts all state and local laws. National Labor Relations Act §§ 1–19 (1935), 29 U.S.C. §§ 151–169 (2018); see also Schwartz, supra note 21, at 928 (discussing the NLRA’s legislative challenges because of its preemption provisions).
\item \textsuperscript{23} See Schwartz, supra note 21 (discussing the different ways lawmakers can design preemption provisions of federal laws); see also Danielle K. Citron, The Privacy Policymaking of Attorneys General, 92 Notre Dame L. Rev. 747, 801–03 (2016) (explaining preemption of state law and the role of state attorneys general (“AG”) in privacy enforcement generally). The GLBA is an example of a federal law that establishes a minimum level of legal protections and requirements and allows for states to impose more stringent laws. Gramm-Leach-Bliley Act of 1999 (“GLBA”), 15 U.S.C. § 6807 (2018).
\item \textsuperscript{24} 15 U.S.C. § 6807.
\item \textsuperscript{25} See Citron, supra note 23 (explaining preemption of state law and the role of state attorneys general in privacy enforcement).
\item \textsuperscript{26} Id.
\item \textsuperscript{27} See Gruwell, supra note 20 (discussing the significance of preemption in the privacy debate).
\end{itemize}
data privacy laws, as states have taken varying approaches to consumer protection by adopting a patchwork of legislation.

The California Consumer Privacy Act ("CCPA") is currently the most protective comprehensive state data privacy law in the country. As of October 2019, sixteen other states have introduced comprehensive state privacy bills to enhance consumer data protections of their residents. Many state data privacy bills give consumers a private right of action. Other state laws provide for consumers' rights to access personal information collected and shared with third-parties, to deletion of their data, to data portability, and to opt out of the sale of personal information. Additionally, as of October 2019, twelve state privacy laws, including the CCPA, require covered entities to provide privacy notices. The CCPA and ten other state laws prohibit discrimination against consumers who exercise their privacy rights.


32. See Lauren Davis, Note, The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation, 24 N.C. BANKING INST. Part V (2020) (discussing the effect of the CCPA on financial institutions' privacy compliance efforts).

33. See Noordyke, supra note 30 (tracking state data privacy efforts); see also Lazzarotti et al., supra note 4 (explaining changes in state data privacy laws).


35. See Noordyke, supra note 30 (evaluating state data privacy proposals).

36. See id. (discussing trends among state data privacy legislation).

37. See id. (analyzing state data privacy proposals).
privacy bills further impose unique obligations on companies, such as mandatory data privacy assessments38 and fiduciary duty requirements.39

Some argue that federal privacy legislation should not preempt state laws because each state serves as a “laboratory” of democracy that experiment with innovative approaches to protect its citizens.40 However, a uniform federal regulatory approach would be more appropriate because of “the inherently interstate nature of electronic commerce and associated data breaches.”41 Preemption is crucial to the federal data privacy law debate because one federal law would greatly simplify industry compliance efforts in the long run by establishing uniform national standards.42

Further, a federal standard would ensure that consumers receive the same privacy rights and data protections regardless of where they may live.43 Privacy legislation should balance the convenience gained from preempting state laws against the potential loss of strong consumer protections afforded by state data privacy laws.44 To serve both the interests of the banking industry and its consumers, lawmakers should enact a comprehensive federal data privacy law with robust consumer

---


protections that expressly preempts existing state data privacy laws.\textsuperscript{45} Therefore, a federal data privacy law should include the most protective aspects of state laws to avoid watering down consumer protections.\textsuperscript{46}

Conversely, opponents argue that a broadly preemptive federal privacy law would be difficult to enact and amend.\textsuperscript{47} An expressly preemptive federal privacy law would be difficult to enact because preemption is a divisive issue that lawmakers have not been able to settle.\textsuperscript{48} Furthermore, a preemptive federal law would be challenging to amend because industry stakeholders and consumer advocates could get congressional support and interfere with efforts to change it.\textsuperscript{49} However, one way to combat this is to include a “sunset provision”\textsuperscript{50} that would allow legislators to consider the law’s effectiveness and address issues that may have arisen since implementation.\textsuperscript{51} For example, the Fair Credit Reporting Act (“FCRA”) contained a series of sunset provisions.\textsuperscript{52} When those sunset provisions neared expiration, Congress amended the FCRA with the Fair and Accurate Credit Transactions Act in 2003 to increase the law’s protections.\textsuperscript{53} A sunset provision that sets a time limit on federal preemption can serve as “a safeguard against regulatory ossification”\textsuperscript{54} in the face of rapidly changing technologies.\textsuperscript{55}

\textsuperscript{45} See id. (advocating for comprehensive consumer protections in future federal data privacy legislation).

\textsuperscript{46} See Chin & Odell, supra note 28 (“While some panelists positioned a preemptive federal law as beneficial for both businesses and consumers, through setting clear and uniform rules across the nation; they also emphasized that any preemptive law would need to be substantial enough to protect consumers.”); see also Levitt & Keller, supra note 44 (discussing the need for privacy legislation to have strong protections like the CCPA to avoid a watered-down bill that gives the appearance of protecting consumers).

\textsuperscript{47} See Gruwell, supra note 20 (discussing the significance of preemption in the privacy debate); Schwartz, supra note 21, at 928 (addressing the challenges of preemptive federal laws).

\textsuperscript{48} Schwartz, supra note 21, at 928 (explaining the obstacles lawmakers face to enact preemptive federal data privacy legislation).

\textsuperscript{49} Additionally, such legislation would likely “become outdated as technological changes undermine such a statute’s regulatory assumptions.” See id. at 946.

\textsuperscript{50} A sunset provision is a provision that will expire after a certain amount of time. See id. at 946 (addressing sunset provisions in the context of preemption).

\textsuperscript{51} See id. at 945 (discussing sunset provisions as a way to draft preemptive statutes).

\textsuperscript{52} Id.

\textsuperscript{53} Id. at 946.

\textsuperscript{54} Ossification “means a lack of meaningful changes over time within and without [the federal statute] in response to new conditions” as it relates to a federal statute’s preemption of state laws. Id. at 928 (citation omitted).

\textsuperscript{55} Id. at 946.
B. Amending the GLBA

The U.S. has a sectoral approach to federal privacy regulation, which means that privacy laws only apply to certain industries, like the GLBA’s application to financial institutions. 56 Although consumers of financial institutions have benefitted from the GLBA’s privacy protections, the Act has come under scrutiny. 57 To comply with the GLBA, financial institutions must “respect the privacy of its customers and . . . protect the security and confidentiality of those customers’ nonpublic personal information.” 58 The GLBA defines consumers’ “nonpublic personal information” to be “personally identifiable financial information” that a financial institution obtains related to providing a financial product or service to an individual, unless that data is otherwise available to the public. 59

Despite the GLBA’s privacy protections, the Act’s narrow scope excludes other kinds of personal information collected and used by financial institutions, information that should be protected as well. 60 For example, financial institutions gather information about visitors to their websites or mobile applications for visits unrelated to financial services or opening of an account. 61 Banks may then use that consumer data internally for marketing purposes and externally by selling that information to third parties. 62 Additionally, the GLBA does not protect information connected to data use related to marketing or data analytics. 63

56. See Developing the Administration’s Approach to Consumer Privacy, Notice of Request for Public Comments, 83 Fed. Reg. 187, 48602 (proposed Sept. 26, 2018) (“For users of products and services in several sectors (e.g., healthcare, education, financial services), specific laws cover how organizations handle personal information. Where no sector-specific laws apply, the Federal Trade Commission (FTC) has the authority to ensure that organizations are not deceiving consumers or operating unfairly.”).


59. Id. § 6809(4); 12 C.F.R. §§ 1016.1–.17 (2018) (setting forth the CFPB’s financial privacy rule, Regulation P, which regulates banks privacy practices).

60. See Dembosky et al., supra note 57 (addressing the consequences of the CCPA on privacy practices of financial institutions).

61. Id.

62. See id. (explaining information that falls outside of the CCPA’s GLBA exemption).

63. See id. (discussing the effects of the CCPA on financial institutions subject to the GLBA and their compliance considerations). Data analytics involves analyzing raw data using algorithms to draw conclusions about that data. Avantika Monnappa, Data Science Vs.
The Act excludes information about financial institutions’ job applicants, contractors, and employees. Further, while the GLBA ensures that customers have an opportunity to “opt out” of data transfers to unaffiliated parties of financial institutions, it provides multiple exceptions to the opt-out requirement that allow financial institutions to ignore a customer’s request to not have her data transferred to non-affiliates.

Future federal legislation should address the shortcomings of the GLBA either by amending the GLBA provisions related to data privacy, providing carve-outs for GLBA provisions related to data privacy, or doing a combination of both. For instance, lawmakers could adopt a compromised approach to provide robust protections for consumers and ease compliance challenges. This approach could preempt state laws, like the CCPA, while incorporating the CCPA’s approach to defining personal information and providing a limited carve-out for the GLBA.

The CCPA provides a GLBA exemption for financial institutions subject to GLBA data protection requirements. Such a compromised approach would allow banks to continue complying with the GLBA’s privacy provisions while requiring them to satisfy the parts of the CCPA that protects consumer data not covered by the GLBA.

---

64. Dembosky et al., supra note 57.
66. Rubin, supra note 11.
67. Based on amendments to the CCPA in September 2018, the CCPA provides entities covered by the GLBA a limited exemption by exempting from the CCPA “personal information collected, processed, sold or disclosed” under the GLBA and its implementing regulations. California Consumer Privacy Act of 2018 (“CCPA”), CAL. CIV. CODE § 1798.145(e) (West 2018).
68. See Schwartz, supra note 21, at 904 (addressing different approaches lawmakers can take to address preemption).
69. Id.
70. See infra Part III for analysis of the definition of personal information.
71. Schwartz, supra note 21, at 904; see also Dembosky et al., supra note 57 (explaining the CCPA-related compliance challenges that financial institutions will face).
72. CAL. CIV. CODE § 1798.145(e).
73. See Dembosky et al., supra note 57 (addressing challenges financial institutions will face under the CCPA).
Although tracking GLBA-covered information makes compliance more difficult for financial institutions, banks should weigh those difficulties against the ease of compliance of a federal data privacy law which preempts state laws. Ultimately, a strong comprehensive federal privacy law should replace the aspects of the GLBA that relate to data privacy only if it provides consumers with stronger protections.

III. AMENDMENT OF THE INFORMATION AND ENTITIES COVERED UNDER THE GLBA

In order to justify preemption of state data privacy laws and amending the GLBA’s privacy provisions, future data privacy legislation should include clear and all-encompassing definitions of the data and entities covered. Broad definitions under federal data privacy legislation will protect a large swath of consumer personal data and ensure that preemption of state laws does not erode consumer protections. Because federal regulators have suggested implementing a risk-based data privacy framework, which would implement safeguards based on the sensitivity of the information, lawmakers should extend this concept to the definitions of personal information. Federal privacy legislation should distinguish between sensitive and non-sensitive personal information in their definitions of personal information. The scope of the definition of personal information is important, as it will affect how companies engage in commercial activity and innovation. Therefore, lawmakers should balance a broad definition of personal information with tiers of privacy requirements based on the sensitivity of consumer information.

This approach of providing protections based on the risk level of data is a calculated method of balancing compliance costs against

74. Financial institutions should recognize that a uniform regulatory approach to all categories of personal information would better protect their consumers. See id. (discussing the effects of the CCPA on financial institutions and compliance considerations).
75. See id. (explaining CCPA compliance challenges).
76. See id. (evaluating the effects of data privacy legislation on financial institutions).
77. See id. (comparing the scope of CCPA and GLBA).
79. Id.
80. Id.
81. Id.
consumer benefits.\textsuperscript{82} Researchers have noted that increased privacy protections do not necessarily lead to increased digital trust and use by consumers.\textsuperscript{83} Consequently, legislators should not require the industry to provide the same high level of protection to both sensitive and non-sensitive data because such an approach would unnecessarily overburden financial institutions.\textsuperscript{84}

Current legislative proposals, however, have provided limited definitions of information covered.\textsuperscript{85} The Information Transparency and Personal Data Control Act\textsuperscript{86} ("Data Control Act") defines sensitive information as "information relating to an identified or identifiable individual," including government created identification, verification credentials, call records, biometric data, sexual preferences, and religion.\textsuperscript{87} "Sensitive information" excludes behavioral information, such as a user’s web and app usage, geolocation data, and email address.\textsuperscript{88} Slightly more inclusive than the Data Control Act, the Social Media Privacy Protection and Consumer Rights Act of 2019\textsuperscript{89} ("Consumer Rights Act") defines personal information more broadly as "individually identifiable information about an individual collected online."\textsuperscript{90} This definition includes nonpublic personal information under the GLBA,\textsuperscript{91}
protected health information under the Health Information Portability and Accountability Act of 199692 (“HIPAA”), and location information that would identify the name of a consumer’s street and a city, a physical address, an email address, and a telephone number.93 Although the Consumer Rights Act protects more kinds of consumer personal data, legislators should ensure that a future definition of personal information is expansive enough to protect consumers across a sufficient range of business activities.94

Furthermore, a federal data privacy law should define and address sensitive personal data as a subset of personal information that should receive additional protections, similar to the Data Control Act and the Balancing the Rights of Web Surfers Equally and Responsibly Act of 201995 (“BROWSER Act”).96 Both bills provide separate definitions and protections for sensitive personal information, which is information that personally identifies an individual, and non-sensitive personal information, which is anonymized or publicly available data.97 However, both the BROWSER Act and the Data Control Act afford little protection for non-sensitive personal information.98 Non-sensitive personal information should receive protection under a preemptive federal data privacy law because many consumers value the privacy of their non-sensitive information as well.99 A distinction between sensitive personal data and personal information will help ensure that the financial services industry is efficiently protecting its consumers’ data.100

In order to preempt other laws without significantly reducing consumer protections, Congress should consider the most expansive definition of covered data currently at the state-level, which is presently the definition of “personal information” under the CCPA.101 The

94. Id.
96. The BROWSER Act states that it would not supersede any existing federal privacy laws; therefore, if this bill passes, financial institutions would have to continue to comply with the GLBA. Id.
98. FED. TRADE COMM’N, supra note 78.
99. Id.
100. Id.
101. California Consumer Privacy Act of 2018 (“CCPA”), CAL. CIV. CODE § 1798.140(o)(1) (West 2018); see Davis, supra note 32 (addressing the impact of the CCPA on financial institutions).
CCPA’s definition covers “information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

Therefore, the CCPA’s expansive scope applies to nearly every kind of information a business could collect about an individual. Federal privacy legislation should include such an expansive definition of personal data. Although compliance with this definition will be challenging for financial institutions, it is a worthwhile compromise to avoid the substantial difficulties banks would otherwise face navigating a patchwork of state laws with varying requirements and definitions of covered data.

IV. USER CONSENT AND USER RIGHTS TO ACCESS, WITHDRAW, CORRECT, AND DELETE

User consent is a common theme across legislative proposals, and federal data privacy legislation should include a robust user control and consent framework. User control and consent is a fundamental aspect of establishing and maintaining consumer trust. Consumers of

102. CAL. CIV. CODE § 1798.140(o)(1).
104. See id. (discussing compliance challenges presented by CCPA).
105. See id. (addressing legal issues presented by the CCPA and the GLBA).
107. See FED. TRADE COMM’N, supra note 78 (analyzing the benefits of the notice and consent framework to provide transparency and a degree of user control in the context of digital privacy).
the financial services industry should expect all industry stakeholders to offer control over their data. This requirement across industries will increase consumer trust in online activities, an important source of economic opportunity. Many companies provide privacy protections that generally require some degree of consent from consumers for a company’s ability to use consumer information, and this can take the form of “opt-in consent” or “opt-out consent.”

Opt-in consent is a stronger method of consumer control and requires affirmative action by a user to explicitly grant a company permission to use the consumer’s information. For example, opt-in consent often consists of a user clicking on a checkbox next to a statement that says “I agree to the Terms of Use and Privacy Policy.” or on a button that says “I agree to the Terms of Use and Privacy Policy.” On the other hand, opt-out consent is passive consent, such that a consumer’s consent to a company’s use of the consumer’s information is presumed, unless the consumer affirmatively objects. Opt-out consent could take the form of a user unchecking a pre-checked box next to a statement of agreement to undo the user’s assumed affirmation, or providing users with the option to withdraw consent by clicking on a link, such as the ubiquitous “unsubscribe” link in marketing emails.

Future federal data privacy should require companies to provide consumers with the ability to opt out of businesses’ use of non-sensitive personal data and to seek additional opt-in consent for sensitive consumer data. The Data Control Act, for instance, requires that companies, by

---

109. See Fed. Trade Comm’n, supra note 78 (addressing the benefits of the providing user control over personal data in the context of digital privacy).
110. See Conroy et al., supra note 108 (explaining the importance of trust for commercial activity online).
112. Id.
113. Id.
114. Id.
115. Id.
116. See Bernard, supra note 10 (arguing for a comprehensive federal data privacy law).
default, obtain opt-in consent for collecting, using, or sharing users’
sensitive personal information, while providing users the right to opt out
of sharing their non-sensitive personal information.\textsuperscript{117}\textsuperscript{117} Unlike other bills,
the Data Control Act provides a “reasonable expectation of users”
exception to the “opt-in consent” requirement.\textsuperscript{118}\textsuperscript{118} Pursuant to this
exception, companies need not obtain such consent for the use of
“sensitive personal information or behavioral data” where this use “does
not deviate from purposes consistent with a [company’s] relationship
with users as understood by the reasonable user.”\textsuperscript{119}\textsuperscript{119} This carve-out is so
expansive that it could defeat the opt-in consent requirements’s protective
purpose—companies could use it to cover their actions beyond data use
related to their operations.\textsuperscript{120}\textsuperscript{120} Legislators should exercise caution in
providing such broad exemptions because a preemptive federal data
privacy law should not create gaps that weaken consumer rights to opt in
or opt out of sharing personal data.\textsuperscript{121}\textsuperscript{121}

Consumers should have the ability to control their personal data
with options to access, withdraw, correct, and delete their personal
data.\textsuperscript{122}\textsuperscript{122} Existing federal sectoral privacy laws\textsuperscript{123}\textsuperscript{123} and state laws\textsuperscript{124}\textsuperscript{124}
already recognize the importance of providing consumers such rights. While the
provision of these rights may seem daunting to companies, they have
symbolic value that help strengthen companies’ relationships with their

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{117} Data Control Act, H.R. 2013, 116th Cong. § 3 (2019).
  \item \textsuperscript{118} Id.
  \item \textsuperscript{119} Id.
  \item \textsuperscript{120} Id.; see also Levitt & Keller, supra note 44 (recommending consumer privacy protections for federal data privacy legislation).
  \item \textsuperscript{121} See id. (discussing consumer privacy protections for federal data privacy legislation).
  \item \textsuperscript{122} See Mark Sullivan, As Google Turns 20, It Can’t Take Our Goodwill for Granted, FAST COMPANY (Sept. 27, 2018), https://www.fastcompany.com/90243161/as-google-turns-20-it-cant-take-our-goodwill-for-granted [https://perma.cc/48GX-TQTS] (discussing the importance of transparency of consumer data).
  \item \textsuperscript{123} See 45 C.F.R. §§ 164.524, 164.526 (2018) (outlining patient rights to request a copy of protected health information and to amend protected health information under the privacy rule of the HIPAA); But see 12 C.F.R. § 1016.1 (2018) (providing consumers the right to opt out of sharing nonpublic personal information but does not provide consumers any right to correct or receive a copy of nonpublic personal information under the GLBA’s Regulation P).
\end{itemize}
\end{footnotesize}
customers, particularly when companies use and share consumer data to engage in marketing and to maintain partnerships with third party service providers.125

Although no federal legislative proposal provides consumers the right to correct information about themselves, industry and regulatory stakeholders generally support this right.126 Additionally, the proposed Consumer Rights Act 127 and several state laws128 provide consumers the right to delete their data.129 Some federal data privacy proposals130 provide users with the right to access the information a company has about them and to withdraw consent provided earlier, which many industry stakeholders support.131 If federal data privacy legislation is to preempt state laws, legislators should include these various rights to control data to ensure a sufficiently robust federal privacy law that provides rights comparable to those offered at the state level.132

---

125. Sullivan, supra note 122.
126. Developing the Administration’s Approach to Consumer Privacy, Notice of Request for Public Comments, 83 Fed. Reg. 187, 48602 (proposed Sept. 26, 2018) (outlining the Administration’s privacy goals and recommending that companies should provide reasonable control to users, including the right to correct consumer information in certain circumstances); Framework for Consumer Privacy Legislation, BUS. ROUNDTABLE 4 (Dec. 2018), https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf [https://perma.cc/JA46- 4DBQ] (proposing user controls, such as the right to correct, in federal privacy legislation).
127. The Consumer Rights Act limits this right to instances where a user deletes their account or otherwise terminates use of a company’s platform. Social Media Privacy and Consumer Rights Act of 2019, S. 189, 116th Cong. (2019). Additionally, the Consumer Rights Act allows consumers to request a company delete their personal information after a company experiences a privacy breach. Id.
128. See, e.g., CAL. CIV. CODE §§ 1798.100–1798.198.
129. Developing the Administration’s Approach to Consumer Privacy, 83 Fed. Reg. at 48602 (recommending that companies should provide reasonable control to users, which includes the right to access, withdraw, correct, and delete consumer information in certain circumstances); Framework for Consumer Privacy Legislation, supra note 126, at 4 (“Consumers should be able to require an organization to delete their personal data collected by an organization, when such data is no longer required to be maintained under applicable law or is no longer necessary for legitimate business purposes of the organization.”).
131. Developing the Administration’s Approach to Consumer Privacy, Fed. Reg. at 48601 (advocating user data control rights); Framework for Consumer Privacy Legislation, supra note 126, at 3 (proposing inclusion of user controls in future data privacy legislation).
uniform set of rights will provide consumers control without overburdening companies and interfering with their operations.133

V. ENFORCEMENT AUTHORITY

A. The FTC and State Attorneys General

Although other federal agencies may currently enforce the privacy provisions of federal sectoral privacy laws, such as the CFPB’s enforcement of the GLBA’s Regulation P,134 stakeholders strongly support making the FTC the primary enforcer of a federal data privacy law.135 Because of the FTC’s experience and existing role in protecting data privacy across many industries, supporters argue that the FTC is best positioned to enforce a comprehensive federal privacy law that would apply across all industries.136 The FTC uses its general authority under Section 5 of the Federal Trade Commission Act of 1914 (“FTC Act”) to protect consumers from unfair and deceptive trade practices.137 In the data privacy sphere, the FTC considers whether companies are engaging in unfair and deceptive practices by using consumer data in a manner that conflicts with the companies’ published privacy policies or related public

---

133. FED. TRADE COMM’N, supra note 78.

134. If legislators provide carve-outs for existing sector-specific federal privacy laws, such as the GLBA, under a comprehensive federal privacy law, then federal agencies, such as the CFPB, will continue to enforce the privacy provisions of their respective sector-specific privacy laws. See supra Part II (discussing amendment of the GLBA).


136. See Developing the Administration’s Approach to Consumer Privacy, Fed. Reg. at 48602 (addressing the role of the FTC in future data privacy enforcement efforts).

statements and whether companies are not delivering on their promises to safeguard personal data from unauthorized use.138

The FTC principally uses enforcement actions139 against organizations that fail to protect consumers’ privacy and personal data as a way to end the unlawful behavior and to compel violators to remEDIATE their illegal actions.140 For example, an FTC order can require companies to adopt privacy and security programs, to conduct biennial assessments by independent assessors to ensure compliance with settlement terms, or to offer consumers tools for transparency and choice.141 Additionally, the FTC may obligate companies to compensate harmed consumers, disgorge unlawful financial gains, or delete consumer data obtained unlawfully.142

However, the FTC’s limited ability to issue civil penalties restricts its ability to enforce data privacy measures.143 Furthermore, the FTC does not have civil penalty authority144 under Section 5 of the FTC Act, meaning the FTC cannot impose direct civil penalties on organizations for first-time violations of Section 5 of the FTC Act.145 The FTC may only seek civil penalties when an entity has violated a consent order, a statute, or rule that explicitly provides for civil penalty authority.146

138. See U.S. Gov’t Accountability Off., supra note 135, at 9–10 (explaining how the FTC enforces data privacy).
139. The FTC’s data privacy enforcement activities consist of litigation and consent decrees, similar to a settlement agreement. See id. (mentioning the different accountability mechanisms the FTC uses in its data privacy efforts).
141. Fed. Trade Comm’n, supra note 140.
142. Id.
143. See U.S. Gov’t Accountability Off., supra note 135, at 1 (explaining restraints on FTC enforcement powers).
144. See id. at 10, n.23 (“Civil penalty authority gives an agency the ability to seek a monetary remedy from an entity that has violated a statute or regulation.”).
145. Id. at 20.
146. Id. at 10.
Federal data privacy legislation should remedy this enforcement gap by providing the FTC authority to impose civil penalties on companies for first-time violations of Section 5. Proponents state that the FTC’s current financial payment and fining regime does not impose high enough costs to adequately discourage bad behavior. Many businesses currently consider these FTC payments “a cost of doing business.” Civil penalties are a concrete method to keep companies accountable to the law and will have an amplified deterrent effect on companies in conjunction with the other payments the FTC can require from violators.

In addition to FTC enforcement, federal data privacy legislation should consider extending state Attorney General (“AG”) authority to bring enforcement actions on behalf of their residents. Some legislative proposals include provisions granting AGs such authority. Supporters of AG enforcement authority argue that enforcement authority should not be too centralized and overburden one regulator, especially considering the increased enforcement workload that will inevitably result from a new federal privacy law. Furthermore, AGs are likely better equipped than the FTC to represent their residents’ interests in litigation. AGs can effectively draw upon prior experience

147. Id. at 35.
148. Id.
149. Id.
150. See id. (explaining the role of penalties in FTC enforcement efforts); But see FED. TRADE COMM’N, supra note 78 (“[T]he FTC Act today does not include civil penalties for first-time violations [because] . . . [y]ou cannot marry an incredibly broad law that is incredibly vague with the ability to impose penalties upon a company that simply fails to predict where a line is drawn.”).
151. Meyer, supra note 135.
153. See Meyer, supra note 135 (“There’s no way that one agency, even an emboldened and better funded FTC, can really deal with what’s going on [in terms of data practices in the marketplace].”) (quotation omitted); FED. TRADE COMM’N, supra note 78 (“[W]e really want a situation where there’s lots of different regulators, like attorneys general, state attorneys generals who are empowered to do the kinds of investigations that we need to have real transparency and real accountability.”); Citron, supra note 23, at 799 (“Federal authorities cannot attend to most privacy and security problems because their resources are limited and their duties ever expanding.”).
154. See Meyer, supra note 135 (“[W]hen cases involve granular, geolocation-based personalization or where the data practices of a mom-and-pop store are in question, it makes sense for the states to play an important role.”); see e.g., Cary Silverman & Jonathan L. Wilson, State Attorney General Enforcement of Unfair or Deceptive Trade Acts and Practices Laws: Emerging Concerns and Solutions, 65 KAN. L. REV. 209, 257 (2016) (“Now, with increased storage of consumer data and a rise in security breaches, state attorneys general and
enforcing data privacy protections in their states as well as their local expertise.\(^{155}\) Although opponents worry that AG involvement may lead “to over-enforcement [that] overwhelms companies,”\(^{156}\) AG enforcement is important to ensure that consumers’ interests are adequately protected under a federal privacy law that preempts state privacy laws.\(^{157}\) Otherwise, consumers would lose a large source of existing protection through AG enforcement activity under the current regime.\(^{158}\)

\[\text{B. Private Right of Action}\]

While some states provide consumers with a private right of action, most notably the CCPA,\(^{159}\) none of the current federal legislative proposals offer this source of accountability to allow consumers to take companies to court for federal privacy law violations.\(^{160}\) A private right of action is a legal mechanism that increases corporate liability and further incentivizes companies to follow data privacy law.\(^{161}\) Yet, some critics of a private right of action consider FTC enforcement alone to be more effective in keeping companies accountable than private law claims.\(^{162}\) These critics also state that private rights of action will lead to frivolous litigation that will hinder innovation in the marketplace and reduce resources that companies could use to safeguard consumer privacy.\(^{163}\)
Despite these critiques, Congress should ultimately incorporate a limited private right of action because tailored language and careful drafting can alleviate opponents’ concerns about frivolous litigation. Lawmakers can draft a narrow private right of action through statutory design by limiting private lawsuits to breaches of certain kinds of personal data, such as sensitive data. Additionally, lawmakers can impose statutory damages for violations of certain provisions of the federal privacy law that are easier to comply with, like data access rights, rather than for violations of any provision of the law. Legislators can also consider requiring that plaintiffs show tangible harm or even imposing an element of intent for statutory violations, such as willful violations. A limited private right of action can reduce industry concerns about frivolous litigation while providing strong consumer protections to justify preemption of existing privacy laws by a future federal data privacy law.

A multi-level enforcement regime through state, federal, and private enforcement activity will help correct existing litigation challenges related to private law claims based on privacy harm. Courts impose high standards for plaintiffs to prove privacy harm and often

(footnotes)
164. Hendel & Lima, supra note 29 (“Privacy advocates like the Electronic Frontier Foundation say Republican concerns about excessive lawsuits can be addressed by careful legislative drafting . . . .”).


166. Id.

167. However, privacy advocates argue that lawmakers should not limit redress for privacy violations to “requiring a showing of a monetary loss or other tangible harm and [instead] should make clear that the invasion of privacy itself is a concrete and individualized injury.” Public Interest Privacy Legislation Principles, https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf [https://perma.cc/DD8Z-P3CH] (last visited Oct. 19, 2019).

168. Jerome, supra note 165 (addressing limitations that lawmakers can impose on a private right of action in future federal privacy legislation).

169. See Hendel & Lima, supra note 29 (“What would make the most sense is to have a strong enforceable federal law[, said California state Sen. Hannah-Beth Jackson.

170. See also Citron, supra note 23 (discussing benefits of enforcement authority shared between federal regulators and AGs in context of data privacy).
dismiss claims based on lack of “injury in fact.” As a result, courts make it difficult for plaintiffs to succeed in privacy tort claims, negligence claims, contract claims, and private claims based on state unfair and deceptive trade acts and practices law.

Strong enforcement mechanisms help incentivize companies to follow a future privacy law. If a future federal privacy law will, in fact, serve as the baseline for consumer privacy protections, legislators should include public enforcement by the FTC and AGs and a limited private right of action in data privacy legislation.

VI. CONCLUSION

Preemption of state law may be a key component of effective federal privacy legislation. Notwithstanding the benefits of preemption, lawmakers should only include a provision that preempts state privacy laws if the federal privacy bill includes other essential elements. These elements include a broad definition of personal data, robust user control rights, expanded FTC powers, AG enforcement rights, and a limited private right of action. Otherwise, federal privacy legislation that lacks these safeguards and preempts existing state laws is “a watered-down bill that gives the appearance of protecting consumers.” Ultimately, lawmakers will need to combine these key elements with other important protections to create a robust federal privacy bill.

171. See id. at 798 (explaining difficulties injured consumers face in pursuing privacy-related litigation); see, e.g., In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014) (finding claimant failed to present “injury in fact”).
172. See Citron, supra note 23, at 798 (addressing challenges for plaintiffs bringing privacy torts such as “intrusion on seclusion, public disclosure of private fact, false light, and misappropriation of image . . . .”).
173. Id.
174. See Hendel & Lima, supra note 29 (addressing private right of action in federal privacy law as an effective legal mechanism for accountability).
175. See Fed. Trade Comm’n, supra note 78 (considering important issues and protections that lawmakers must consider for federal privacy legislation); see also Hendel & Lima, supra note 29 (addressing consumer protections to include in future federal privacy law).
176. See Schwartz, supra note 21, at 945 (explaining various approaches to preemption in context of privacy law).
177. Id.
178. See Fed. Trade Comm’n, supra note 78 (evaluating consumer protections that legislators should include in federal data privacy law).
179. See Levitt & Keller, supra note 44 (explaining data privacy provisions that future federal legislation should include like a private right of action); see also Schwartz, supra note 21, at 945 (discussing different perspectives on preemption of state data privacy laws).
points to strike a balance between robust consumer protections and flexibility for companies to continue their operations and to innovate. 180

Future data privacy law should include mechanisms for companies to provide transparency and control to consumers over their personal data without being overly prescriptive in how companies should achieve these goals. 181 For instance, legislators should draft a provision that requires companies to publish a data use policy that is easy for the average person to understand, as the Data Control Act does. 182 Like the Data Control Act, this privacy policy requirement should also compel companies to explain the ways in which they will use consumer data. 183 Regulators, consumer advocates, and academics can hold companies accountable by analyzing companies’ detailed, but easy-to-follow privacy policies on behalf of consumers. 184 Additionally, lawmakers should consider providing privacy protections for a broad range of consumer data while differentiating between sensitive data and non-sensitive data. 185

Legislators should also avoid concentrating all enforcement powers in one agency and should instead consider distributing enforcement authority between the FTC, state AGs, and consumers through a private right of action. 186 Overcentralization of power can overburden the enforcing agency and lead to limited enforcement activity by the agency. 187 Based on its experience in the data privacy sphere, the FTC should be the main enforcement agency under any future federal

---

180. See Fed. Trade Comm’n, supra note 78 (analyzing consumer rights that legislators should include in federal privacy proposals).

181. Id.; Developing the Administration’s Approach to Consumer Privacy, Fed. Reg. at 48601 (explaining the benefits of a flexible outcome-based approach to privacy regulation).


184. See Fed. Trade Comm’n, supra note 78 (explaining the benefits of privacy policies to the public).

185. Id. (discussing the benefits of distinguishing between sensitive and non-sensitive information in context of providing privacy protections).

186. Supra Part V; see also Citron, supra note 23, at 798 (“State enforcers are essential to the efficient deterrence of privacy and data security violations given the increasing marginalization of private law and the practical constraints on federal agencies.”).

187. See Citron, supra note 23, at 799–800 (explaining the limits the FTC faces in its privacy enforcement activities).
privacy law. Nevertheless, state AGs should also have the power to bring enforcement actions on behalf of their residents to ensure robust enforcement. Finally, wronged consumers should be able to engage in external accountability through an appropriately limited private right of action that can prevent nuisance litigation. Ultimately, a comprehensive federal privacy law that establishes strong, uniform protections for data privacy will benefit industries like the financial services sector by providing certainty, maintaining consumer trust, and avoiding stifling industry innovation.

Although federal data privacy legislation will certainly ease the burden of compliance on financial institutions by bringing uniformity on a national level, this will not resolve all privacy issues. Because many financial services organizations must comply with the GDPR currently, a comprehensive federal data privacy law will create compliance challenges. With the addition of U.S. federal legislation, companies will have to navigate a new international patchwork of laws. Uniformity of data privacy law at the national and international level would be ideal in light of the borderless nature of the Internet. Nevertheless, U.S. lawmakers should begin by establishing a national standard that strikes a balance between protecting consumer data,

188 Supra Part V.
189 Supra Part V.
190 Supra Part V.
191 See BUS. ROUNDTABLE, supra note 1 (discussing the support of industry stakeholders, including financial institutions, for the enactment of comprehensive federal privacy legislation).
194 See Feld, supra note 4 (evaluating GDPR impact on U.S. financial institutions).
industry innovation, and the freedom of small businesses. This will mean selecting beneficial parts of the GDPR to incorporate into federal legislation, such as consumer rights to control their data, and discarding other parts, like the GDPR’s rigid fine structure. U.S. lawmakers should avoid overwhelming U.S. industries with a burdensome data privacy framework as stringent as the GDPR.

FARA SOUBOUTI*

196. See Schulze, supra note 193 (explaining GDPR consequences for U.S. companies).
197. See id. (addressing the compliance challenges associated with privacy law).
198. Id.; But see Tung, supra note 195 (evaluating the effects of the GDPR’s robust data privacy protections on the industry).

* I would like to thank all of my wonderful family and friends for their constant support and understanding throughout the process of developing this Note. I am incredibly grateful to Professor Lissa L. Broome, Morgan O. Schick, Brianne Marino Glass, T. Nute Thompson, Devon R. Tucker, and the staff members of the North Carolina Banking Institute Journal for their thoughtful edits and comments which guided me to the final stages of the publication process.