SETTLING DATA PROTECTION LAW: MULTISTATE ACTIONS AND NATIONAL POLICYMAKING

Elysa M. Dishman

SETTLING DATA PROTECTION LAW: MULTISTATE ACTIONS AND NATIONAL POLICYMAKING

*Elysa M. Dishman**

Data privacy and cybersecurity law in the United States is as unsettled as it is unsettling. By failing to pass comprehensive data protection legislation, Congress has settled for uncertainty. And the authority of the Federal Trade Commission (FTC) to enforce and seek remedies in this area has been challenged by litigants, including a case currently pending in the U.S. Supreme Court. Nevertheless, FTC enforcement settlements play a vital role in data regulation. These settlements include corporate structural reforms that become de facto regulations by shaping corporate practices nationwide.

State attorneys general (AGs) have become increasingly prominent data policymakers through enforcement settlements. AGs have instigated a series of high-profile multistate actions in response to data breaches. Like FTC settlements, multistate settlements also regulate data practices nationwide by requiring corporations to undergo structural reforms. FTC and multistate settlements have distinct differences that are outgrowths of their institutional attributes and enforcement authority that give them each comparative data enforcement advantages. The FTC and AGs may also engage in "borrowing" one another's enforcement strengths to augment their power to regulate by settlement. As a result, the future of data protection regulation will likely be shaped by more aggressive federal and multistate settlements, rather than by comprehensive legislation or agency rulemaking.

And that is unsettling. Courts and commentators have raised concerns about regulation by settlement. But those concerns have not been considered in light of the rise of multistate enforcement actions. Unique attributes of multistate enforcement exacerbate existing concerns about regulation by settlement, and at the same time, raise entirely new ones. This Article explores how AGs can continue to play an important role in data protection policymaking while reducing concerns about regulation via multistate settlement.

INTRODUCTION

In 2019, Facebook and the Federal Trade Commission (FTC) announced a record-breaking $5 billion settlement for data privacy violations that occurred in the wake of the Cambridge Analytica scandal.[1] But for Facebook CEO Mark

* Elysa M. Dishman is an Associate Professor at BYU Law. She would like to thank the participants of the 2019 ComplianceNet Conference, Rocky Mountain Jr. Scholars Conference, and the 2020 BYU Law Work-in-Progress Series for their helpful comments. She would also like to thank Tyler Kivley, Vivian Tse, and Brandon Bourg for their valuable research assistance.

1. After news broke that Cambridge Analytica had harvested millions of Facebook users' data without their permission, the FTC began investigating the social media company for potential violations of its 2012 FTC consent decree, in which Facebook agreed it would not share users' information without their consent. *See* Natasha Singer, *Why the F.T.C. is Taking a New Look at Facebook Privacy*, N.Y. TIMES, Dec. 22, 2018. Facebook settled with the FTC in July 2019. *See FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [hereinafter FTC Facebook Press Release]. AGs also have pending investigations based on the Cambridge Analytica incident. *See* Tony Romm, *D.C. Attorney General's Lawsuit Against Facebook Can Proceed, Judge Rules*, WASH. POST, June 1, 2019; Press Release, N.Y. Off. Att'y Gen., Statement from A.G. Schneiderman on Facebook/Cambridge Analytica (Mar. 20, 2018), https://ag.ny.gov/press-release/2018/statement-ag-schneiderman-facebook cambridge-analytica.

Zuckerberg, "even more important" than the $5 billion penalty was that Facebook was "going to make some major structural changes to how we build products and run this company."[2] Some of the structural changes included establishing an independent privacy committee of the board of directors and requiring compliance certifications by Zuckerberg and compliance officers for which they are personally, criminally, and civilly liable.[3] The Facebook settlement sparked a debate, with some hailing it as meaningful corporate reform[4] and others lamenting it was nothing more than "a slap on the wrist."[5] For its part, Facebook stated that these changes go beyond anything required by U.S. law today, "and we hope [they] will be a model for the industry."[6]

U.S. data privacy and security law[7] has been likened to the Wild West,[8] despite the importance of data and technology in the modern economy. Unlike the European Union, the United States lacks a comprehensive federal data protection law.[9] Instead, U.S. data protection law is a "hodgepodge of various constitutional protections, federal and state statutes, torts, regulatory rules, and treaties."[10] Scholars, politicians, and commentators have criticized this approach and made repeated calls for Congress to take action and pass omnibus federal data protection legislation.[11] But instead Congress has settled for

2. *See* Colin Stretch, *FTC Agreement Brings Rigorous New Standards for Protecting Your Privacy*, FACEBOOK (July 24, 2019), https://newsroom.fb.com/news/2019/07/ftc-agreement.

3. *See* FTC Facebook Press Release, *supra* note 1.

4. *See* FED. TRADE COMM'N, STATEMENT OF CHAIRMAN JOE SIMONS AND COMMISSIONERS NOAH JOSHUA PHILLIPS AND CHRISTINE S. WILSON *IN RE FACEBOOK, INC.* (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf.

5. *See* Henry Kenyon, *Democrats Slam Potential Facebook FTC Settlement, Threaten Legislation*, CONG. Q. ROLL CALL (July 15, 2019); FED. TRADE COMM'N, DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA *IN RE FACEBOOK, INC.* (2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

6. *See* Stretch, *supra* note 2.

7. For purposes of this Article, I refer to data security and data privacy collectively as "data protection" as used by Professors Hartzog and Solove in their seminal article. *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2232 (2015).

8. *See* Joe Nocera, *The Wild West of Privacy*, N.Y. TIMES (Feb. 24, 2014), http://www.nytimes.com/2014/02/25/opinion/nocera-the-wild-west-of-privacy.html?_r=0; Cathy O'Neil, *How America Can Stop Being the Wild West of Data*, BLOOMBERG (Aug. 5, 2018), https://www.bloomberg.com/opinion/articles/2018-08-05/how-america-can-stop-being-the-wild-west-of-data.

9. Many scholars have contrasted the sectoral nature of data regulation in the United States to the European Union model which has comprehensive data privacy regulation. *See generally* Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461 (2016); Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29 CONN. J. INT'L L. 257 (2013); Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771 (2019).

10. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

11. *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 137 (2017); Carol Li, Note, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 NOTRE DAME L. REV. 2211, 2231 (2019); Alexis Collins et al., *FTC Commissioners Continue Calls for National Data Privacy and Security Legislation*, CLEARY GOTTLIEB (May 29, 2019), https://www.clearycyberwatch.com/2019/05/ftc-commissioners-continue-calls-for-national-data-privacy-and-security-legislation; *FTC Testifies on Private Sector*

uncertainty, leaving data regulation and enforcement to a haphazard patchwork of federal agencies and states.[12]

More by default than design, the FTC has become the primary federal agency that oversees data protection. The bulk of the FTC's consumer protection enforcement, including its data protection enforcement, is pursuant to its powers under Section 5 of the Federal Trade Commission Act (FTC Act), which broadly prohibits "unfair and deceptive acts or practices."[13] The FTC does not engage in formal rulemaking to regulate data practices under its Section 5 authority.[14] The lack of rulemaking is because the FTC does not have Administrative Procedure Act (APA) rulemaking authority under Section 5 of the FTC Act.[15] Instead, the FTC must meet heightened standards to engage in formal rulemaking.[16] Instead of engaging in rulemaking, the FTC heavily relies upon enforcement as its primary vehicle to regulate corporate data practices.[17] In fact, FTC enforcement settlements are so important to developing data practices that scholars have referred to the body of settlements as the "Common Law of Privacy."[18]

The FTC's reliance on enforcement to regulate data practices has resulted in corporate targets challenging the FTC's authority and its ability to seek certain remedies. Even though courts have upheld the FTC's data enforcement authority under Section 5, the FTC remains vulnerable to claims that its

Data Privacy Before Senate Homeland Security and Government Affairs Subcommittee, FED. TRADE COMM'N (Mar. 7, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-testifies-private-sector-data-security-senate-homeland; Katie Zezima, *Obama Proposes Legislation on Data Breaches, Student Privacy*, WASH. POST (Jan. 12, 2015), https://www.washingtonpost.com/news/post-politics/wp/2015/01/12/obama-to-propose-legislation-on-data-breaches-student-privacy.

12. Proposed comprehensive data privacy legislation has come before Congress in recent years, but none has gained significant traction so far. *See* Wendy Zhang, *Comprehensive Privacy Law Still Pending*, JDSUPRA (Jan. 10, 2020), https://www.jdsupra.com/legalnews/comprehensive-federal-privacy-law-still-66167. Congressional Democrats and Republicans are divided on whether proposed legislation should include a private cause of action and preempt state data protection laws. *Id.* For a discussion of recent data privacy proposed legislation, see Joanna Kessler, Note, *Data Protection in the Wake of the GDPR: California's Solution for Protecting: "The World's Most Valuable Resource,"* 93 S. CAL. L. REV. 99, 124–26 (2019); Susan Steinman, *A Plethora of Privacy Bills*, 56 AM. ASS'N FOR JUST. 54 (2020) ("While it seems unlikely that comprehensive privacy legislation will be enacted this year, pressure will continue to mount on Congress to protect consumers."); Müge Fazlioglu, *Tracking the Politics of US Privacy Legislation*, IAPP (Dec. 13, 2019), https://iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation.

13. 15 U.S.C. § 45.

14. *See* Gerard M. Stegmaier & Wendall Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 692 (2013).

15. *See* Solove & Hartzog, *supra* note 10, at 620.

16. *See* 15 U.S.C. § 57b-3. The FTC has only Magnuson-Moss rulemaking authority under Section 5 of the FTC Act, which is so procedurally burdensome that it is largely ineffective. *See* Solove & Hartzog, *supra* note 10, at 620; Maureen K. Ohlhausen, *The FCC's Knowledge Problem: How to Protect Consumers Online*, 67 FED. COMMC'N L.J. 203, 212 n.46 (2015) (suggesting that the "FTC's process is enforcement-centric rather than rulemaking-centric" because Magnuson-Moss imposes higher procedural burdens on FTC rulemaking).

17. *See* Solove & Hartzog, *supra* note 10, at 587.

18. *Id.* at 627.

settlements are unenforceable because the terms are not sufficiently specific.[19] In addition, the Supreme Court is currently considering the FTC's authority to seek restitution under certain provisions of the FTC Act.[20] Challenges to the FTC's authority create uncertainty about the FTC's ability to regulate data practices and seek restitution in future settlements.

In contrast, states have risen in prominence as powerful national data regulators and enforcers. State legislatures have led the way in passing data protection statutes that have effects far outside their state borders. For example, California passed the California Consumer Privacy Act (CCPA), the most comprehensive privacy statute in the United States, which went into effect in January 2020.[21] Every state legislature in the country has passed data breach notification laws that require companies to notify consumers in the event of a data breach.[22]

States have also regulated data practices through enforcement actions brought by state attorneys general (AGs) against corporations for violations of state and federal data laws.[23] AGs have joined together to form multistate actions in response to high-profile data breaches.[24] AGs are currently pursuing multistate investigations of data breaches at Marriott[25] and eBay[26] and have

19. *See* F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); LabMD, Inc. v. F.T.C., 894 F.3d 1221 (11th Cir. 2018).

20. *See* AMG Capital Mgmt., LLC v. F.T.C., 910 F.3d 417 (9th Cir. 2019), *cert. granted*, 141 S. Ct. 194 (2020); *see also* Recent Case, *Statutory Interpretation—Stare Decisis—Seventh Circuit Uses Methodological Stare Decisis to Review Substantive Precedent*—F.T.C. v. Credit Bureau Center, LLC*, 937 F.3d 764 (7th Cir. 2019)*, 133 HARV. L. REV. 1444, 1445 (2020); M. Sean Royall et al., *Seventh Circuit Sets Up Potential Supreme Court Review on FTC Monetary Relief Authority*, 34 ANTITRUST 54, 54 (2019).

21. *See* California Consumer Privacy Act, CAL. CIVIL CODE § 1798.185 (West 2020); Kessler, *supra* note 12, at 102. Virginia became the second state to pass a comprehensive data statute in March 2021. *See* Rebecca Klar, *Virginia Governor Signs Comprehensive Data Privacy Law*, THE HILL (Mar. 2, 2021), https://thehill.com/policy/technology/541290-virginia-governor-signs-comprehensive-data-privacy-law.

22. *See Security Breach Notification Laws*, NAT'L CONF. STATE LEGIS., https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Feb. 20, 2021).

23. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 756–57 (2016).

24. *See id.*

25. *See* Chris Mills Rodrigo, *New York Attorney General Opens Investigation into Marriott Hacking*, THE HILL (Nov. 30, 2018), https://thehill.com/policy/technology/419104-new-york-attorney-general-opens-investigation-into-marriott-hacking; *AG Paxton Begins Investigation into Marriott Data Breach Affecting 500 Million Customers Worldwide*, TEX. OFF. ATT'Y GEN. (Nov. 30, 2018), https://www.texasattorneygeneral.gov/news/releases/ag-paxton-begins-investigation-marriott-data-breach-affecting-500-million-customers-worldwide [hereinafter Texas AG Marriott Press Release].

26. *See* Ryan Mac, *California Joins Other States in Investigation Of eBay Hack*, FORBES (May 23, 2014), https://www.forbes.com/sites/ryanmac/2014/05/23/as-ebay-notifies-users-of-hack-states-launch-investigation/#68c479b6f278.

settled actions with Home Depot,[27] Equifax,[28] Uber,[29] and Target.[30] Like the FTC, AGs rely on settlements to broadly transmit data standards to corporations by demanding that corporations undergo structural reforms.[31] In this manner, AGs have used multistate settlements to shape corporate practices and data policy nationally.[32]

While scholars have discussed FTC data protection settlements, there has been little attention paid to multistate settlements.[33] This Article is the first to extensively analyze and compare structural reforms in multistate and FTC data protection settlements. FTC and multistate settlements share some similar terms, but they also differ in important ways that are extensions of their attributes and authority.

The FTC and AGs each have comparative advantages in data enforcement and borrow from one another's strengths to augment their power to regulate data practices in settlements.[34] For example, AGs have relied upon established terms in FTC settlements and the FTC's institutional capacity, expertise, and permanence to establish norms and monitor compliance. At the same time, AGs have charted new paths in data enforcement by innovating with structural reforms and other terms in multistate settlements.[35] The FTC can adapt its settlement terms based on multistate innovations and shore up its authority by

27. *See* Angela Morris, *States Score $17.5M Settlement From Home Depot Over 2014 Data Breach*, LAW.COM (Nov. 24, 2020), https://www.law.com/texaslawyer/2020/11/24/states-score-17-5m-settlement-from-home-depot-over-2014-data-breach/?slreturn=20210225155500.

28. *See Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FED. TRADE COMM'N (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [hereinafter FTC Equifax Press Release].

29. *See Attorney General DeWine Announces $148 Million Multistate Settlement with Uber*, OHIO OFF. ATT'Y GEN. (Sept. 26, 2018), https://www.ohioattorneygeneral.gov/Media/News-Releases/September-2018/Attorney-General-DeWine-Announces-$148-Million-Mul [hereinafter Ohio AG Uber Press Release].

30. *See A.G. Schneiderman Announces $18.5 Million Multi-State Settlement with Target Corporation Over 2013 Data Breach*, N.Y. OFF. ATT'Y GEN. (May 23, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over [hereinafter New York AG Target Press Release].

31. *See* Donald G. Gifford, *Impersonating the Legislature: State Attorneys General and Parens Patriae Product Litigation*, 49 B.C. L. REV. 913, 944 (2008); Paul Nolette, *State Attorneys General Are More and More Powerful. Is That a Problem?*, WASH. POST (Mar. 5, 2015), https://www.washingtonpost.com/news/monkey-cage/wp/2015/03/05/state-attorneys-general-are-more-and-more-powerful-is-that-a-problem ("AG-led lawsuits have become a crucial part of the American regulatory landscape, particularly since their resolution often involves millions (even billions) in fines and new regulatory requirements for the targeted industries.").

32. *See* PAUL NOLETTE, FEDERALISM ON TRIAL: STATE ATTORNEYS GENERAL AND NATIONAL POLICYMAKING IN CONTEMPORARY AMERICA 215 (2015); Citron, *supra* note 23, at 791.

33. *See* Citron, *supra* note 23, at 791; Colin Provost, *An Integrated Model of U.S. State Attorney General Behavior in Multi-State Litigation*, 10 STATE POL. & POL'Y Q. 1, 2 (2010) ("Multi-state litigation deserves scholarly attention because its dynamics are still poorly understood, yet the key players involved believe . . . it has had profound effects on regulatory governance.").

34. *See* Elysa M. Dishman, *Enforcement Piggybacking and Multistate Actions*, 2019 BYU L. REV. 421, 421 (2019).

35. *See* Citron, *supra* note 23, at 756–57.

relying on states' stronger enforcement authority and data protection laws.[36] Borrowing empowers the phenomenon of regulation by settlement. As a result, the future of data protection regulation will likely be shaped by more aggressive federal and multistate settlements rather than by comprehensive legislation or agency rulemaking. And that is unsettling.

Courts and commentators have raised concerns about regulation through enforcement settlements in general and specifically in the context of FTC data enforcement settlements.[37] Regulation by settlement refers to the practice of enforcers setting de facto regulations by requiring settlement terms with a corporation that are then followed by the rest of the industry.[38] Agencies have the ability to choose the method of regulation whether it is through rulemaking or adjudication, including informal disposition through settlement.[39] Regulation by settlement bypasses traditional checks on policymaking that are more participatory and transparent, such as the legislative process, rulemaking, and judicial review.[40] Regulation by settlement has also been criticized as vague.[41] Both litigants and scholars have argued that the FTC's settlement terms are too vague to provide fair notice, raising due process concerns.[42]

Regulation by multistate settlement raises similar concerns as its federal equivalent. However, unique attributes of multistate enforcement exacerbate those concerns and raise entirely new ones. Multistate settlements also sidestep checks in the policymaking processes, but they do so in ways that are even less participatory and transparent than their federal agency counterparts.[43] Multistate settlements are negotiated behind closed doors with little involvement from outside stakeholders.[44] Even though many states may participate in a multistate action, it is actually only a few leading AGs that negotiate the settlement.[45] The few leading AGs are democratically accountable to their own state electorates but not to a broader group of affected

36. *See* Gregory James Evans, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Beaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 192–93 (2015).

37. *See* Lisa Shultz Bressman, *Beyond Accountability: Arbitrariness and Legitimacy in the Administrative State*, 78 N.Y.U. L. REV. 461, 473 (2003); Brandon Garrett, *The Public Interest in Corporate Settlements*, 58 B.C. L. REV. 1483, 1486 (2017); Matthew C. Turk, *Regulation by Settlement*, 66 U. KAN. L. REV. 259, 262 (2017).

38. *See* Turk, *supra* note 37, at 260.

39. *See* Sec. & Exch. Comm'n v. Chenery Corp., 332 U.S. 194, 196 (1947).

40. *See* Steven M. Davidoff & David Zaring, *Regulation by Deal: The Government's Response to the Financial Crisis*, 61 ADMIN. L. REV. 463, 468 (2009); Turk, *supra* note 37, at 323.

41. *See* Turk, *supra* note 37, at 318; Bressman, *supra* note 37, at 542; Stegmaier & Bartnick, *supra* note 14, at 697.

42. *See* Justin Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 1002–06, 1018 (2016); Steigmaier & Bartnick, *supra* note 14, at 697; Jennifer L. West, *A Case of Overcorrection: How the FTC's Regulation of Unfair Acts and Practices Is Unfair to Small Businesses*, 58 WM. & MARY L. REV. 2105, 2130–32 (2017).

43. *See* Gifford, *supra* note 31, at 944.

44. *See* NOLETTE, *supra* note 32.

45. *See id.* at 26; Elysa M. Dishman, *Class Action Squared: Multistate Actions and Agency Dilemmas*, 96 NOTRE DAME L. REV. 291, 291 (2020); Provost, *supra* note 33.

stakeholders.[46] Further, unlike FTC settlements, multistate settlements do not have to comply with notice and comment procedures designed to increase transparency and participation.[47]

Multistate settlements are also particularly vulnerable to the criticism that they evade judicial review. State courts play a limited role overseeing multistate settlements. Some states' statutes do not require court approval for settlements at all.[48] In states that do require court approval, courts are often deferential to settlements proposed by AGs and do not provide meaningful review.[49] In contrast, settlements with federal agencies like the FTC are subject to administrative court and federal district court review.[50]

Institutional concerns have been raised about AGs as national data policymakers.[51] AGs are generalist enforcers with limited resources whose offices may lack the institutional capacity to create national policy, especially in areas that require technological expertise.[52] AGs may not be well-positioned to be national policymakers when they are only democratically accountable to their state residents.[53] And ambitious AGs seeking re-election or election to higher office may prioritize headlines and large penalties over creating meaningful and cohesive corporate structural reforms.[54]

Multistate settlements can also interject greater uncertainty about data compliance into national policy.[55] State regulation of data protection creates a patchwork of regulations that create uncertainty for regulated entities.[56] Multistate actions are made up of ad hoc groups of states, and settlements can include different and potentially conflicting provisions—making it difficult to

46. Forty-three of the nation's AGs are elected statewide separately from the governor or other state institutions. William P. Marshall, *Break Up the Presidency? Governors, State Attorneys General, and Lessons from the Divided Executive*, 115 YALE L.J. 2446, 2448 n.3 (2006). State AGs are appointed in the other seven states: Alaska, Hawaii, Maine, New Hampshire, New Jersey, Tennessee, and Wyoming. *Id.* In Maine, the attorney general is selected by the state legislature and in Tennessee by the state supreme court. *Id.* In the other five states, Alaska, Hawaii, New Hampshire, New Jersey, and Wyoming, the attorney general is appointed by the governor. *Id.*

47. *See A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last updated Oct. 2019) [hereinafter *Overview of FTC Authority*].

48. Rather, state courts may only require that the settlement be filed in state court or not filed at all. *See* Dishman, *supra* note 45, at 347.

49. *See id.*; Garrett, *supra* note 37; Margaret H. Lemos, *Aggregate Litigation Goes Public: Representative Suits by State Attorneys General*, 126 HARV. L. REV. 486, 510 n.105 (2012).

50. *See Overview of FTC Authority*, *supra* note 47.

51. *See* Lemos, *supra* note 49; Dishman, *supra* note 45, at 305.

52. *See* Tara L. Grove, *When Can a State Sue the United States*, 101 CORNELL L. REV. 851, 897–98 n.225 (2016) (citing NAT'L ASS'N OF ATT'YS GEN., STATE ATT'YS GENERAL: POWERS AND RESPONSIBILITIES 47–49, 84 & n.1 (Emily Myers ed., 3d ed. 2013)).

53. *See* Amanda M. Rose, *State Enforcement of National Policy: A Contextual Approach (With Evidence from the Securities Realm)*, 97 MINN. L. REV. 1343, 1372 (2013).

54. *See* Lemos, *supra* note 49, at 515 n.123.

55. *See* Turk, *supra* note 37, at 319 (identifying a multienforcer problem with regulation by settlement).

56. *See* Kristin N. Johnson, *Managing Cyber Risks*, 50 GA. L. REV. 547, 577 (2016); Schwartz & Peifer, *supra* note 11, at 135–36.

harmonize the settlements into a cohesive policy. Multistate settlements have greater variation in their terms than FTC settlements. It is unclear how multistate settlements should be interpreted together because the identity and number of states participating in settlements is in flux.

While there are concerns about shaping national policy through multistate settlements, AGs have provided an important service to consumers by instigating greater data protections.[57] AGs have stepped into a void where the FTC and private enforcers have faced obstacles in data protection enforcement.[58] This Article explores how AGs can continue to play an important role in data protection policymaking while reducing concerns about regulation through multistate settlement.

This Article proceeds in three parts. Part I discusses the FTC and AGs as distinct data enforcers. Part II analyzes and compares structural reforms in FTC and multistate data protection settlements. Part III discusses the implications of regulating by multistate settlement and makes recommendations on how to improve this unique form of regulation.

I. A TALE OF TWO DATA PROTECTION ENFORCERS

The FTC and AGs are distinct data enforcers. While both enforcers have statutory authority to bring consumer protection actions based on "unfair or deceptive acts or practices,"[59] challenges to the FTC's enforcement authority, constraints on the agency's rulemaking power, and limitations on its ability to demand civil penalties weaken the FTC's ability to regulate and enforce data violations. In contrast, AGs' data enforcement authority remains virtually unchallenged.[60] Several other factors have also empowered AGs to rise as national data enforcers and policymakers.

57. *See* Citron, *supra* note 23; Hurwitz, *supra* note 42, at 957 ("Since the advent of the consumer Internet, there has been a palpable regulatory vacuum in these areas."); *see also* Prentiss Cox et al., *Strategies of Public UDAP Enforcement*, 55 HARV. J. ON LEGIS. 37, 39 n.8 (2018) (quoting Myriam Gilles & Gary Friedman, *After Class: Aggregate Litigation in the Wake of* AT&T Mobility v. Concepcion, 79 U. CHI. L. REV. 623, 660 (2012)).

58. For a discussion of the limitations of common law torts actions for data breaches, see Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J. F. 614, 619–24 (2018).

59. *Overview of FTC Authority*, *supra* note 47; 15 U.S.C. § 45(a)(2).

60. Benjamin A. Powell et al., *FTC Investigations and Multistate AG Investigations*, GLOB. INVESTIGATIONS REV. (June 19, 2019), https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/first-edition/article/ftc-investigations-and-multistate-ag-investigations ("[T]he dearth of regulations and case law provides substantial power to the State AGs on how [UDAP statutes] are to be interpreted.").

A. Federal Trade Commission

More by default than design, the FTC has become the primary federal data protection agency enforcer in the United States.[61] The FTC is an independent federal agency.[62] Its mission is to protect consumers by "preventing anticompetitive, deceptive, and unfair business practices."[63] Except for a few small industry carve-outs, almost every industry is subject to FTC enforcement power.[64] This means that nearly any industry that affects consumers is within the scope of FTC enforcement power.

1. FTC Data Enforcement Authority

The bulk of FTC data enforcement occurs pursuant to its broad power under Section 5 of the FTC Act that prohibits "unfair or deceptive acts or practices."[65] Rather than attempt to list and define specific acts in violation of the statute, Congress created two broad categories: 1) practices that are deceptive and 2) practices that are unfair.[66]

The FTC began its data enforcement under Section 5 by bringing actions against companies for engaging in "deceptive practices"[67] based on misrepresentations in their data privacy policies.[68] By focusing on voluntary, affirmative statements in company privacy policies, the FTC used a largely self-regulatory approach to build a foothold in the area of data protection.[69] However, an obvious shortcoming of this approach was that companies could

61. *See* Hartzog & Solove, *supra* note 7, at 2245 ("When Congress created the Federal Trade Commission . . . , it never imagined the Commission would become the primary agency responsible for grappling with technological change, but that's precisely what the FTC has become: the de facto Federal Technology Commission.") (citing *Now in its 100th Year, the FTC has Become the Federal Technology Commission*, TECH FREEDOM (Sept. 26, 2013), https://techfreedom.org/now-in-its-100th-year-the-ftc-has-become-the).

62. *Human Capital Management Office*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/human-capital-management-office (last visited Feb. 20, 2021). "The [FTC] is headed by five Commissioners, nominated by the President and confirmed by the Senate[.] . . . No more than three Commissioners can be of the same political party. The President chooses one Commissioner to act as Chairman." *About the FTC, Commissioners*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/commissioners (last visited Feb. 20, 2021).

63. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Feb. 20, 2021).

64. This includes "industries such as automotive, financial, health, retail, online services, hospitality, entertainment, manufacturing, data processing, food and beverage, transportation, and many more." Hartzog & Solove, *supra* note 7, at 2236; *see also* 15 U.S.C. § 45(a)(2).

65. 15 U.S.C. § 45(a)(2).

66. *See id.*

67. A deceptive practice under Section 5 is defined as a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." Solove & Hartzog, *supra* note 10, at 599.

68. *See id.* at 598–99; Hurwitz, *supra* note 42, at 965; David Alan Zetoony, *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for Its Breaches*, 2011 STAN. TECH. L. REV. 12 (2011).

69. *See* Solove & Hartzog, *supra* note 10, at 604.

effectively opt out of FTC oversight by not making representations in their privacy policies or not having privacy policies at all.[70]

The FTC grew concerned about the conduct of companies outside their stated privacy policies and sought to expand its enforcement to create data security standards under its "unfairness" authority.[71] Unreasonable data security practices may be considered "unfair practices" under Section 5 when they result in a data breach.[72] The FTC has increasingly brought data enforcement actions pursuant to its unfairness authority under Section 5.

The FTC is hampered in its ability to regulate by rulemaking because of the heightened rulemaking procedural requirements under Section 5. The FTC's rulemaking authority under Section 5, commonly referred to as Magnuson-Moss rulemaking, includes more cumbersome rulemaking requirements than the more widely known APA process.[73] As a result, the FTC has not engaged in Magnuson-Moss rulemaking under its Section 5 authority. The FTC has urged Congress to grant it APA rulemaking power under Section 5 in order to keep up with changes in technology.[74]

While Section 5 makes up the bulk of FTC data enforcement, the FTC has enforcement and rulemaking powers related to data protection from a host of other federal statutes.[75] For example, the FTC has APA rulemaking power and enforcement authority under the Gramm-Leach-Bliley Act (GLBA)[76] and the Children's Online Privacy Protection Act (COPPA).[77] The FTC has engaged in

70. *See* Hurwitz, *supra* note 42.

71. *See id.* An unfair practice under Section 5 "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). To be unfair, conduct must (1) cause substantial injury, (2) without offsetting benefits, which (3) consumers cannot avoid. *See* Hurwitz, *supra* note 42, at 965.

72. *See, e.g.*, F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); LabMD, Inc. v. F.T.C., 894 F.3d 1221 (11th Cir. 2018).

73. *See* 15 U.S.C. § 57a(a)(1)(B); *see also* Stegmaier & Bartnick, *supra* note 14. For example, Magnuson-Moss rulemaking requires "provid[ing] . . . for an informal hearing" where interested parties are entitled to present oral testimony and potentially cross examine witnesses. 15 U.S.C. § 57a(b)–(c).

74. *See* FED. TRADE COMM'N, FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY 7–8 (2020), https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf ("[T]argeted authority to enact privacy rules under the APA would better allow us to ensure that the law keeps up with changes in technology.").

75. There is also overlapping enforcement authority among federal agencies in the area of data protection. For example, the FTC has concurrent authority to enforce the Fair Credit Reporting Act (FCRA) and consumer protection laws with the Consumer Protection Financial Bureau (CPFB). *See Consumer Finance*, FED. TRADE COMM'N https://www.ftc.gov/news-events/media-resources/consumer-finance (last visited Feb. 20, 2021).

76. *See* 15 U.S.C. § 6804(a)(1)(C) (rulemaking authority); 15 U.S.C. § 6805(a)(7) (enforcement authority). The GLBA safeguard requirements mirror the FTC's requirements for a comprehensive "information security program." 16 C.F.R. § 314.4 (2020).

77. *See* 15 U.S.C. § 6502(b) (rulemaking authority); 15 U.S.C. § 6505(a) (enforcement authority).

formal rulemaking[78] and has brought enforcement actions under those statutes.[79]

2. FTC Enforcement Investigations and Settlements

FTC enforcement actions typically begin with an investigation. The FTC "may initiate an enforcement action . . . if it has 'reason to believe' that the law is being or has been violated."[80] The FTC may abandon an investigation if the agency decides that it does not warrant further enforcement action.[81] Generally, investigations are non-public, and the investigation only becomes public when a settlement is announced.[82] However, on occasion the FTC will announce an investigation in a press release prior to settlement.[83] Given the FTC's limited resources, the agency tends to target cases with a high likelihood of success where companies have no viable defense.[84]

FTC settlements are most commonly in the form of consent decrees.[85] FTC consent decrees legally function like contracts between parties rather than as binding precedent applicable to third parties.[86] However, Professors Solove and Hartzog have influentially argued that the FTC's consent decrees form a "Common Law of Privacy."[87] FTC consent decrees involve case-by-case adjudication with published outcomes that provide notice and some level of

78. *See* Christine S. Wilson, Comm'r, Fed. Trade Comm'n, Opening Remarks at FTC Workshop: The Future of the COPPA Rule 9 (Oct. 7, 2019) (transcript available at https://www.ftc.gov/system/files/documents/public_statements/1547693/wilson_-_ftc_coppa_workshop_opening_remarks_10-7-19.pdf).

79. *See, e.g.*, Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief at 2, United States v. Musically, No. 2:19-cv-01439 (C.D. Cal. 2019) (COPPA); Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. PLS Fin. Servs., Inc., No.1:12-cv-08334 (N.D. Ill. 2012) (GLBA, FCRA).

80. *See Overview of FTC Authority*, *supra* note 47.

81. *See, e.g.*, Letter from David Vladeck, Fed. Trade Comm'n, to Albert Gidari, Perkins Coie LLP (Oct. 27, 2010) (available at https://www.ftc.gov/sites/default/files/documents/closing_letters/google-inquiry/101027googleletter.pdf).

82. *See* Solove & Hartzog, *supra* note 10, at 623.

83. *See, e.g.*, *Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Rights*, FED. TRADE COMM'N (March 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

84. *See* Solove & Hartzog, *supra* note 10, at 613.

85. However, investigations may end in a default judgment or abandonment of the action by the FTC in the investigatory stage. *See id.* at 606.

86. 1 STEPHANIE W. KANWIT, FED. TRADE COMM'N § 12:6 (2013) ("[A]ny other interpretation would hamper the consent settlement process.").

87. Solove & Hartzog, *supra* note 10, at 676. The FTC has also referred to its consumer protection efforts relating to privacy and data security as developing a "common law" body of rules. Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at George Mason University School of Law 17th Annual Antitrust Symposium: Unfair Methods and the Competitive Process: Enforcement Principles for the Federal Trade Commission's Next Century 7 (Feb. 13, 2014) (transcript available at https://www.ftc.gov/system/files/documents/public_statements/314631/140213section5.pdf).

precedent.[88] Consent decrees are designed to have "a huge impact on other businesses in the same industry or that use similar practices."[89] The FTC relies heavily on settlements to signal the basic rules that it wants companies to follow.[90] This means that "[p]erhaps the single most important and widely applying body of precedent that regulates privacy in the United States is not in the form of any traditional kind of privacy law, such as cases or statutes."[91] FTC consent decrees are not strictly precedential in the sense that the FTC is required to follow them in the future, but the FTC has striven to be consistent.[92]

There are several procedural requirements for FTC consent decrees. Before it can be finalized, a proposed consent decree is publicly available for comment for thirty days before it becomes final.[93] The Commission responds to those who comment on proposed orders.[94] Commissioners vote to approve settlement orders and may write concurring and dissenting statements to reflect their views on the action.[95] "When the FTC issues a settlement, it typically issues a complaint and settlement document simultaneously, and these are publicized on the FTC's website."[96] The complaints contain allegations that form the factual basis for the consent decrees. These complaints usually allege violations of Section 5 "due to a combination of failing to have an information security policy, implement system monitoring, fix known vulnerabilities, maintain firewalls and updated antivirus software, use encryption, implement intrusion detection and prevention solutions, store information only as long as necessary, and prepare for known or reasonably foreseeable attacks."[97]

The FTC is limited in its ability to seek civil penalties for violations of Section 5. In general, Section 5 does not allow the FTC "to seek civil penalties for a first-time offense."[98] Thus, most of FTC data protection consent decrees contain no civil penalties because most involve first-time offenders. The FTC is largely limited to assessing civil penalties only after a company has violated its pre-existing consent decree.[99] Companies that violate their consent decrees

88. Solove & Hartzog, *supra* note 10, at 621. Others have challenged Professors Solove and Hartzog's characterization of FTC enforcement as common law. *See* Hurwitz, *supra* note 42, at 971.

89. Solove & Hartzog, *supra* note 10, at 624.

90. *See id.*

91. *Id.* at 588, 607 ("In the world of privacy law practice, everything the FTC says and does is delicately parsed, like the statements of the Chairman of the Federal Reserve.").

92. *Id.* at 620.

93. *Overview of FTC Authority*, *supra* note 47; 16 C.F.R. § 2.34(c).

94. *See, e.g.*, *Equifax Information Services LL* [sic], FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/102-3252/equifax-information-services-ll (Mar. 15, 2013) (providing FTC responses to public comment).

95. *See, e.g.*, FTC Facebook Press Release, *supra* note 1.

96. Solove & Hartzog, *supra* note 10, at 621.

97. Stegmaier & Bartnick, *supra* note 14, at 693.

98. *See* Solove & Hartzog, *supra* note 10, at 605; FED. TRADE COMM'N, *supra* note 74, at 7.

99. For example, the FTC's fine against Facebook was based on the violation of a previous order. FTC Facebook Press Release, *supra* note 1.

are liable for a civil penalty of up to $16,000 per violation.[100] In most instances, there is no threat of financial penalties for violating Section 5, and there is little financial incentive for corporations to spend a great deal of time and resources fighting the FTC's enforcement actions.[101] Settling with the FTC also allows companies to "eliminate the uncertainty and expense of lengthy negotiation and pretrial preparation and litigation" in addition to preventing reputational damage that can come from a drawn-out enforcement action.[102]

In addition to consent decrees, the FTC has created a form of "'soft law' that consists of guidelines, press releases, workshops, and white papers" that discuss data protection standards.[103] These materials are offered by the FTC as guidance, "yet the FTC has never clearly articulated which parts of its recommendations are mandatory and which parts are simply best practices."[104] Because Section 5 is broad and settlement terms require companies to implement reasonable data programs, FTC guidance plays a significant role in establishing data standards.

3. Challenges and Limitations to FTC Enforcement

Challenges to the FTC's authority and limitations on its enforcement ability weaken and inject uncertainty into its data enforcement. While courts have upheld the FTC's enforcement authority under Section 5, doubts still remain about the extent of the FTC's enforcement powers and the remedies the agency can pursue. The issue of the FTC's power to seek equitable monetary remedies such as restitution under a certain provision of the FTC Act is currently pending in the Supreme Court. Because the FTC relies heavily on adjudication to regulate data practices, "adverse [court] decisions . . . have an outsized effect on [the FTC's] enforcement ability" in the future.[105]

The FTC's data enforcement authority based on unfairness under Section 5 was first significantly challenged in *FTC v. Wyndham Worldwide*. In that case, the FTC brought an enforcement action against Wyndham after three data breaches occurred over a two-year period.[106] The FTC alleged that Wyndham's data security practices were unfair because they were unreasonably insufficient to protect customers' data from third parties.[107] Wyndham argued that the FTC's enforcement authority over unfair business practices did not extend to a

100. *Commission Approves Federal Register Notice Adjusting Civil Penalty Amounts*, FED. TRADE COMM'N (Dec. 23, 2008), https://www.ftc.gov/news-events/press-releases/2008/12/commission-approves-federal-register-notice-adjusting-civil.

101. *See* Hurwitz, *supra* note 42, at 1007.

102. KANWIT, *supra* note 86, at § 12:4.

103. Solove & Hartzog, *supra* note 10, at 625.

104. *Id.* at 626.

105. FED. TRADE COMM'N, *supra* note 74, at 7.

106. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 241–42 (3d Cir. 2015).

107. *Id.* at 240–41.

company's alleged failure to adopt "reasonable and appropriate" data security measures.[108] The Third Circuit rejected Wyndham's argument, holding that the FTC's enforcement authority over unfair practices encompassed data security practices under Section 5 of the FTC Act.[109]

Wyndham further argued that the FTC failed to provide constitutionally adequate notice of what data security practices the company was required to follow.[110] The Third Circuit held that Wyndham had fair notice of the meaning of unfairness under the statute as it related to its data practices.[111] The Third Circuit specifically pointed to the FTC's guidance and prior FTC consent decrees that put Wyndham on notice that its lack of data security protections could constitute unfairness under the statute. [112]

The *Wyndham* case solidified the FTC's unfairness enforcement authority under Section 5 and was an important victory for the FTC, but the agency's authority was again challenged in *FTC v. LabMD*. In *LabMD*, a now-defunct diagnostic lab was the target of an FTC enforcement action when an employee inadvertently shared patients' confidential information.[113] The FTC argued that LabMD's data protections were so inadequate as to render them an "unfair act or practice" under Section 5 of the FTC Act.[114] Unlike most enforcement targets, LabMD refused to settle with the FTC and contested the action through administrative proceedings, including a hearing with an administrative law judge and an appeal to the Commission.[115] LabMD was ultimately unsuccessful in the administrative proceedings, and the FTC issued a cease and desist order.[116] LabMD appealed to the Eleventh Circuit and sought to have the order vacated.[117]

The Eleventh Circuit upheld the FTC's unfairness authority; however, importantly, it vacated the FTC's cease and desist order.[118] The LabMD cease and desist order required that the company establish a "comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[119] The Eleventh Circuit held that the order was not sufficiently

108. Appellant's Opening Brief & Joint App. Vol. 1 at 18, F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (2014) (No. 14-3514), 2014 WL 5106183.

109. *Wyndham*, 799 F.3d at 249.

110. Appellant's Opening Brief & Joint App. Vol. 1, *supra* note 108, at 35.

111. *Wyndham*, 799 F.3d at 256.

112. *Id.* at 256–57.

113. LabMD, Inc. v. F.T.C., 894 F.3d 1221, 1224 (11th Cir. 2018).

114. *Id.* at 1223–24.

115. *Id.* at 1225–27.

116. *Id.* at 1227.

117. *Id.*

118. *Id.* at 1237.

119. *Id.* at 1236.

specific, rendering it unenforceable.[120] The Eleventh Circuit found that the language that required LabMD to have a reasonable "comprehensive information security program" was unclear as to what actions LabMD had to take to comply with the order.[121] With the possibility of penalties and contempt for its violation, the court held the order had to be specific enough that LabMD would know what it had to do to comply.[122]

Even though the Eleventh Circuit upheld the FTC's unfairness authority in *LabMD*, the court's holding casts doubt on the enforceability of past FTC consent decrees.[123] The terms of the cease and desist order that were challenged are common terms that the FTC has used in many of its consent decrees. If the terms of the consent decrees are not sufficiently specific, companies may challenge their enforceability when the FTC later alleges violation of the decrees. This concern is particularly significant because the FTC cannot collect civil penalties in the first instance and must rely on enforcing prior consent decrees to seek civil penalties.

The FTC has also faced litigation challenges regarding its ability to seek restitution as an equitable remedy.[124] The Supreme Court is currently considering a case challenging the FTC's ability to seek restitution under Section 13(b) of the FTC Act.[125] Section 13(b) of the FTC Act authorizes the FTC to seek injunctions to remedy "any provision of law enforced by the Federal Trade Commission."[126] Another provision of the FTC Act, Section 19, specifically empowers the FTC to seek restitution; however, heightened requirements under Section 19 have led the FTC to rely on Section 13(b) when seeking

120. *Id.*

121. *Id.* at 1236–37.

122. *Id.*

123. *See* Julia Whall, Note, *Policing Cyberspace: The Uncertain Future of Data Privacy and Security Enforcement in the Wake of LabMD*, 60 B.C. L. REV. E-SUPP. II-149, II-151, II-163 (2019) (arguing that the LabMD decision introduces "confusion about the scope of the FTC's enforcement authority" and constrains future FTC data remediation efforts).

124. *See* FED. TRADE COMM'N, *supra* note 74, at 7 ("For example, recent decisions questioning our ability to obtain injunctive and monetary relief have allowed opposing parties to challenge the agency's pursuit of that relief, presenting further hurdles in obtaining monetary relief for consumers in this area." (footnote omitted)).

125. *See* AMG Capital Mgmt., LLC v. F.T.C., 910 F.3d 417 (9th Cir. 2019), *cert. granted*, 141 S.Ct. 194 (2020).

126. 15 U.S.C. § 53(b); *see also Overview of FTC Authority*, *supra* note 47. The FTC has stated the following regarding its authority:

> Section 13(b) of the FTC Act authorizes the Commission to seek preliminary and permanent injunctions . . . . In the early and mid-1980s, . . . the Commission argued that the statutory reference to "permanent injunctions" entitled the Commission to obtain an order not only permanently barring deceptive practices, but also imposing various kinds of monetary equitable relief (*i.e.*, restitution and rescission of contracts) to remedy past violations . . . . The courts have uniformly accepted the Commission's construction of Section 13(b), with the result that most consumer protection enforcement is now conducted directly in court under Section 13(b) rather than by means of administrative adjudication.

Solove & Hartzog, *supra* note 10, at 612 n.124.

restitution in enforcement actions.[127] Courts have consistently held that the injunctions referred to in Section 13(b) encompass other equitable remedies such as restitution, obviating the need for the FTC to seek restitution under the more cumbersome Section 19.[128] The Ninth Circuit in *AMG Capital Management, LLC v. FTC*, recently ruled consistent with its precedent that the FTC had authority to seek restitution under its Section 13(b) powers, interpreting the term "injunction" broadly to include other equitable remedies.[129] However, the Seventh Circuit recently overturned its own precedent and reversed course, creating a circuit split on the question.[130] The Seventh Circuit, in *F.T.C. v. Credit Bureau Center, LLC*, held that the term "permanent injunction" under Section 13(b) only allowed the court to issue injunctions and not monetary equitable relief.[131] During oral argument, questions asked by the Justices reflected their doubt about the FTC's authority under Section 13(b) to seek restitution.[132] The Supreme Court's decision will have important ramifications for the FTC's consumer protection enforcement if it becomes more difficult for the FTC to seek restitution pursuant to Section 13(b).[133]

Limiting the FTC's ability to seek restitution could also hamper the FTC's future data protection enforcement. Like other consumer protection cases, the FTC routinely cites its Section 13(b) authority in data protection complaints.[134] For example, the FTC's settlement with Equifax, based on a data breach, included significant consumer restitution under the FTC's Section 13(b)

127. 15 U.S.C. § 57b(a)(1); *see also* Royall et al., *supra* note 20, at 57.

128. *See AMG Capital Mgmt.*, 910 F.3d at 426; Royall et al., *supra* note 20, at 57; CHRIS D. LINEBAUGH, CONG. RESEARCH SERV., WILL THE FTC NEED TO RETHINK ITS ENFORCEMENT PLAYBOOK (PART II)? CIRCUIT SPLIT CASTS DOUBT ON THE FTC'S ABILITY TO SEEK RESTITUTION IN SECTION 13(B) SUITS 2 (Jan. 30, 2020), https://www.hsdl.org/?abstract&did=833858.

129. *See AMG Capital Mgmt.*, 910 F.3d at 426.

130. *See* F.T.C. v. Credit Bureau Center, LLC, 937 F.3d 764, 785–86 (7th Cir. 2019); *see also* FTC v. Abbvie, Inc., 976 F. 3d 327, 374–79 (3d Cir. 2020) (holding that Section 13(b) did not authorize the court to order disgorgement.)

131. *Id. Credit Bureau Center, LLC* was initially consolidated with *AMG Capital Management, LLC* and certiorari was granted for the consolidated cases, but the cases were later unconsolidated, and certiorari was vacated in *Credit Bureau Center, LLC*. *See* Docket Order, FTC v. Credit Bureau Ctr., Dckt. No. 19-825, (Sup. Ct. Nov. 9, 2020), https://www.supremecourt.gov/docket/docketfiles/html/public/19-825.html. *AMG Capital Management, LLC* is currently pending in the Supreme Court.

132. Oral arguments occurred on January 13, 2021. During oral argument, the Justices expressed their doubts about the FTC's authority to compel restitution under Section 13 of the FTC Act. *See* Ronald Mann, *Argument Analysis: Justices Doubt FTC's authority to Compel Monetary Relief*, SCOTUSblog (Jan. 14. 2021), https://www.scotusblog.com/2021/01/argument-analysis-justices-doubt-ftcs-authority-to-compel-monetary-relief. According to one commentator, this case may be the simplest for the Court to decide and its first opinion to be released from the January argument calendar. *Id.*

133. *See* Royall et al., *supra* note 20, at 57; LINEBAUGH, *supra* note 128, at 3.

134. *See, e.g.*, Complaint at 22, In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295 (N.D. Ga. 2019).

authority.[135] The future of the FTC's ability to seek restitution in data protection cases is uncertain in light of the pending Supreme Court case.

B. State Attorneys General

Several factors have contributed to AGs' rise in prominence as national data protection policymakers.[136] These factors include the lack of federal comprehensive data legislation, limitations on the FTC's enforcement powers, delegation of enforcement of federal laws to AGs, the increased sophistication of AG offices, and the increasing trend of multistate actions. State enforcement actions, like their FTC counterparts, are overwhelmingly resolved by settlement.[137]

The lack of comprehensive federal data protection legislation and limitations on FTC enforcement has left a void that AGs are well-positioned to fill by enforcing their state consumer protection laws.[138] AGs have become so entrenched in data enforcement that it is unlikely they will be displaced even if Congress passed comprehensive legislation. While federal legislation could preempt some state data laws, AGs have broad consumer protection enforcement powers that will maintain their presence in data protection enforcement. Furthermore, AGs have the unique authority to bring enforcement actions—called *parens patriae* actions—on behalf of their state citizenry.[139] AGs often bring *parens patriae* actions in the area of data protection under their general consumer protection statutes. With the encouragement of the FTC, states adopted "little FTC Acts" or Unfair Deceptive Acts or Practices (UDAP) laws.[140] Like Section 5 of the FTC Act, these state statutes typically prohibit "unfair and deceptive acts and practices."[141] These statutes are broad, and their interpretation is fluid, allowing AGs to adapt enforcement to new technologies.[142] UDAP laws empower AGs to seek "civil penalties, injunctive relief, and attorneys' fees and costs."[143] AGs' authority to bring data protection actions under their UDAP laws has not been challenged by litigants like the FTC's authority has been in the *Wyndham* and *LabMD* cases. Rather, multistate

135. *See* Royall et. al, *supra* note 20, at 54.

136. *See* Citron, *supra* note 23.

137. *See* Lemos, *supra* note 49, at 527; Prentiss Cox, *Public Enforcement Compensation and Private Rights*, 100 MINN. L. REV. 2313, 2350 (2016).

138. *See* Divonne Smoyer, *The Growing Reach of State Attorneys General Over Data Privacy and Security Breach Incidents*, *in* RECENT TRENDS IN PRIVACY AND DATA SECURITY 173 (2013).

139. *See* Jack Ratliff, *Parens Patriae: An Overview*, 74 TUL. L. REV. 1847, 1850 (2000); Dishman, *supra* note 45, at 294; Lemos, *supra* note 49, at 492.

140. *See* Citron, *supra* note 23, at 754.

141. Cox et al., *supra* note 57, at 38.

142. *See* Smoyer, *supra* note 138, at 174.

143. Citron, *supra* note 23, at 754.

data protection actions have settled without litigation challenging the state's data enforcement powers.

AGs have encouraged state legislatures to gap-fill for the lack of comprehensive federal legislation by promoting the adoption of data protection legislation. They have successfully lobbied their state legislatures to pass state data breach notification laws requiring companies to notify consumers in the event of data breaches.[144] Now every state in the country has a form of data breach notification law, even though there is no federal data breach notification law.[145] AGs have played an important role in keeping breach notification laws up to date and defending them from federal preemption.[146] They have urged state legislatures to pass other data protection statutes.[147] Currently two states, California and Virginia, have comprehensive data statutes and each statute has given their AGs significant powers to interpret and enforce the laws.[148] AGs' offices also issue guidance to businesses on how to comply with state data laws.[149]

Federal statutes are increasingly delegating consumer protection enforcement to states, including data protection enforcement.[150] Many federal statutes provide concurrent enforcement authority to federal agencies and AGs.[151] Federal statutes related to data protection that have given enforcement authority to AGs include the Health Insurance Portability Accountability Act (HIPAA), GLBA, Fair Credit Reporting Act (FCRA), and COPPA.[152] AGs have brought a series of enforcement actions based on federal law in the area of data privacy.[153]

144. *See id.*

145. *See Security Breach Notification Laws*, NAT'L CONF. STATE LEGIS., https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Feb. 7, 2020).

146. *See* Citron, *supra* note 23, at 768.

147. For example, the California AG also took a leading role in the state legislature passing the California Online Privacy Protection Act (CalOPPA) requiring mobile apps to have, among other things, privacy policies. *See* Smoyer, *supra* note 138, at 176.

148. The California CCPA provides the AG the powers of enforcement and to engage in rulemaking and includes a private right of action. The Virginia Consumer Data Protection Act (VCDA) provides the AG the sole ability to enforce the statute and has no private right of action. *See* Gretchen Ramos et. al, *Virginia Enacts Comprehensive Data Privacy Legislation*, THE NAT'L L. REV., March 3, 2021, https://www.natlawreview.com/article/virginia-enacts-comprehensive-data-privacy-legislation.

149. *See, e.g.*, KAMALA D. HARRIS, CAL. DEP'T JUST., CALIFORNIA DATA BREACH REPORT 27 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (noting recommendations by the California AG to improve privacy and security practices to reduce data breaches).

150. *See* NOLETTE, *supra* note 32, at 38–41; Margaret H. Lemos, *State Enforcement of Federal Law*, 86 N.Y.U. L. REV. 698, 715 (2011).

151. *See* Dishman, *supra* note 34, at 421.

152. *See* NOLETTE, *supra* note 32, at 38–41.

153. *See, e.g.*, Proposed Final Judgment and Permanent Injunction, California v. Premera Blue Cross, No. SVC-264783 (Cal. App. Dep't Super. Ct. July 11, 2019) [hereinafter Premera Blue Cross Settlement] (multistate HIPPA enforcement action); Stipulated Order for Permanent Injunction and Civil Penalty Judgment, F.T.C. v. Google, LLC, No. 1:19-cv-02642 (D.D.C. Sept 10, 2019) (combined New York and FTC

AGs' offices have become increasingly sophisticated at handling resource-intensive and complex investigations and litigation, including in the area of data protection.[154] Some AGs' offices have organized consumer protection and data protection units with dedicated attorneys and staff.[155] AG offices have also hired and consulted with data privacy professionals and have provided their staff privacy training and certifications.[156]

The rise of multistate actions has facilitated AGs' increased prominence in data policymaking.[157] Multistate actions allow AGs to pool and leverage resources by bringing enforcement actions together instead of separately.[158] A single state or small group of states, such as an executive committee, typically leads multistate actions.[159] It is often the same states that lead multistate actions.[160] Other states participate in the multistate action in varying degrees with some states contributing nothing more than a signature on a settlement document, essentially free riding on the leadership and resources of other states.[161] States that have the most active data enforcement are California, Connecticut, Illinois, Indiana, Maryland, Massachusetts, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Texas, Vermont, and Washington.[162] "In multistate actions, states [often] file separate lawsuits" in their own state courts, "though offices collaborate on aspects of the proceedings."[163] "States issue similar requests for information, share information through common-interest agreements, and engage in joint negotiations."[164]

Because large-scale data breaches affect residents of many states, data breach actions are particularly well-suited for multistate actions. Furthermore, because many states have similar UDAP laws, states have a fairly uniform statutory basis for multistate actions. AGs have initiated investigations and settled several multistate enforcement actions based on high-profile data breaches. For example, there have been multistate settlements in the wake of

COPPA Action). AGs are required to notify the appropriate federal agency of their actions under these federal statutes, and they must be filed in federal court. *See* Lemos, *supra* note 150, at 708.

154. *See* NOLETTE, *supra* note 32, at 8; Citron, *supra* note 23, at 755.

155. *See* Citron, *supra* note 23, at 756.

156. *See id.* at 755.

157. *See* NOLETTE, *supra* note 32, at 23; Dishman, *supra* note 45, at 299.

158. *See* Dishman, *supra* note 45, at 321; Lemos, *supra* note 49, at 523–25 (noting "[a]ttorneys general have limited budgets and small staffs," but can "achieve some economies of scale by banding together in multistate actions").

159. *See* Dishman, *supra* note 45, at 306–07.

160. For example, New York leads multistate actions at twice the rate as the next most active state. *See* NOLETTE, *supra* note 32, at 26.

161. *See* Dishman, *supra* note 34, at 421; Cox et al., *supra* note 57, at 84 ("Participants may lend nothing more than a signature to a settlement agreement . . . ."); NOLETTE, *supra* note 32, at 26–27 ("Many states participate in multistate litigation, but only a few states typically take a leading role in these efforts.").

162. Citron, *supra* note 23, at 755.

163. *Id.* at 761.

164. *Id.*

data breaches with Home Depot,[165] Equifax,[166] Uber,[167] Neiman Marcus,[168] and Target.[169] There are also pending multistate investigations of data breaches that occurred at Marriott[170] and eBay.[171] AGs often coordinate multistate actions through the National Association of Attorneys General (NAAG). There is a NAAG Privacy Working Group, and group members "hold monthly telephone calls to discuss [data breaches,] best practices[,] and emerging risks."[172] Multistate actions have also been brought in coordination with FTC enforcement actions. The FTC and states have generally had a cooperative relationship in data enforcement.[173]

Like FTC enforcement actions, multistate actions routinely end in settlement.[174] These settlements can take the form of consent decrees or, more commonly, Assurances of Voluntary Compliance (AVC).[175] Some states only require filing the AVC in court, while other states do not require court filing or approval of AVCs.[176] If courts are required to approve AVCs, it is generally a very deferential review, without the court meaningfully examining the settlement.[177] Companies are able to neither admit nor deny wrongdoing in AVCs.[178] "Violators [of AVCs generally] incur no obligations, fines, or penalties unless the attorney general files a lawsuit [to enforce the terms of the AVC] and wins."[179]AGs' unchallenged enforcement authority under state and federal data laws make them uniquely poised to be national data policymakers. Multistate enforcement actions provide AGs a platform to nationally regulate corporate data practices by mandating structural reforms through settlements.

165. *See* Morris, *supra* note 27.

166. *See* FTC Equifax Press Release, *supra* note 28.

167. *See* Ohio AG Uber Press Release, *supra* note 29.

168. *See AG Paxton Announces $1.5 Million Settlement with Neiman Marcus over Data Breach*, TEX. OFF. ATT'Y GEN. (Jan. 8, 2019), https://www.texasattorneygeneral.gov/news/releases/ag-paxton-announces-15-million-settlement-neiman-marcus-over-data-breach.

169. *See* New York AG Target Press Release, *supra* note 30.

170. *See* Texas AG Marriott Press Release, *supra* note 25; Rodrigo, *supra* note 25.

171. *See* Mac, *supra* note 26.

172. Citron, *supra* note 23, at 790.

173. *See* Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address to the National Association of Attorneys General "Federal and State Law Enforcement Cooperation: A Lesson From Baseball" (Mar. 6, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/federal-and-state-law-enforcement-cooperation-lesson-baseball/120305naagspeech.pdf.

174. *See* Lemos, *supra* note 49, at 527; Cox, *supra* note 137, at 2350.

175. AVCs are also known as Assurances of Discontinuance (AODs). For the purposes of this paper, I refer to these types of informal settlement agreements as AVCs. In fact, "[i]n some states, the attorney general must give an entity the chance to sign an . . . AVC, before pursuing litigation." Citron, *supra* note 23, at 761 (internal parentheses omitted); *see also* Powell et al., *supra* note 60.

176. *See, e.g.*, COLO. REV. STAT. § 6-1-110 (2020); VA. CODE. § 59.1-202 (2020).

177. *See* Lemos, *supra* note 49, at 503–04.

178. *See, e.g.*, § 59.1-202 ("Such assurance of voluntary compliance shall not be considered an admission of guilt or a violation for any purpose.").

179. Citron, *supra* note 23, at 806.

II. STRUCTURAL REFORMS IN DATA PROTECTION SETTLEMENTS

The FTC and AGs routinely rely on settlements to resolve data enforcement actions. Both enforcers include structural reforms in their settlements. AGs initially relied heavily on the FTC's framework for structural reforms, especially in combined FTC and multistate settlements. But AGs are increasingly charting new paths for structural reforms in multistate settlements. Different approaches in settlements are an extension of the FTC and AGs institutional attributes and enforcement authority. The FTC and AGs borrow from one another's enforcement strengths to augment their power to regulate through settlement.

A. Elements of FTC Data Settlements

FTC settlements are relatively consistent. These components include 1) injunctions prohibiting certain misconduct, 2) penalties and remedies, 3) structural reforms, and 4) third party assessments and ongoing monitoring.[180] These components generally have the same terms across settlements.

First, FTC settlements include injunctive prohibitions barring the company from engaging in conduct that is the subject of the enforcement action.[181] Prohibitions of future misconduct are important in FTC settlements because if companies violate the injunctive provisions, they may be subject to penalties. Even though future misconduct is prohibited, companies are normally not required to admit they engaged in misconduct in the settlement.[182]

Second, in certain circumstances, settlements will include penalties or restitution for consumers. Even if the FTC does not collect penalties, the FTC may require payment to affected consumers as part of the settlement. For example, in the Equifax settlement, over $300 million was allocated to providing consumer compensation and credit monitoring.[183] Even though the FTC may not initially receive any penalties, the penalties for violating an existing consent decree can be substantial. For example, the historic $5 billion Facebook settlement was based on a violation of a 2012 consent decree between Facebook

180. *See* Solove & Hartzog, *supra* note 10, at 613–19.

181. *Id.* at 614.

182. Consent decrees typically allow defendants to neither admit nor deny liability. *See id.* at 613.

183. FTC Equifax Press Release, *supra* note 28. The Consumer Financial Protection Bureau (CFPB) and a multistate group were also included in the Equifax settlement and received civil penalties as part of the settlement, but the FTC did not receive any civil penalties. *Id.* The CFPB received $100 million, and the states received $175 million. *Id.*

and the FTC.[184] Google paid a $22.5 million penalty to the FTC for violating a prior consent decree.[185]

Third, FTC settlements typically require structural reforms to corporate governance, compliance programs, and data practices. The FTC has a standard set of structural reforms that it routinely includes in its consent decrees. The central feature of structural reforms is that the corporation must implement a comprehensive program for data security or privacy.[186] FTC settlements provide a framework for a comprehensive data program. A corporation must designate a responsible employee to be accountable for the program.[187] The corporation is required to engage in risk assessment, identifying "material internal and external risks to the security, confidentiality, and integrity of Personal Information . . . ."[188] Risk assessment includes considering specific categories of risk such as employee training and management, information systems, and prevention of and response to data attacks.[189] Based on the risk assessment, the corporation must adopt internal safeguards to mitigate those risks.[190] Regular testing or monitoring is also required to determine effectiveness of their adopted safeguards.[191]

Structural reforms in FTC settlements have remained relatively consistent over time; however, the FTC has recently made more aggressive demands for structural reforms. For example, the 2019 Facebook settlement required Facebook to establish a board-level privacy committee.[192] The privacy committee must be independent and nominated by an independent nominating committee outside the control of Facebook CEO, Mark Zuckerberg.[193] Additionally, the settlement requires the appointment of designated compliance officers to be responsible for Facebook's privacy program.[194] These compliance officers must be approved by the independent privacy committee and can only be removed by that committee.[195] The compliance officers and Zuckerberg are

184. FTC Facebook Press Release, *supra* note 1.

185. *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMM'N (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

186. *See, e.g.*, Decision and Order, In the Matter of BLU Products, Inc., Docket No. C-4657 (Sept. 6, 2018) [hereinafter BLU Settlement] (requiring a comprehensive security program); Decision and Order, In the Matter of Uber Technologies, Inc., Docket No. C-4662 (Oct. 25, 2018) [hereinafter FTC Uber Settlement] (comprehensive privacy program).

187. *See, e.g.*, BLU Settlement, *supra* note 186, at 4–5; FTC Uber Settlement, *supra* note 186, at 3.

188. *See, e.g.*, BLU Settlement, *supra* note 186, at 5.

189. *See, e.g.*, Stipulated Order for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Ruby Corp., No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016) [hereinafter Ashley Madison Settlement].

190. *See id.*

191. *See id.*

192. FTC Facebook Press Release, *supra* note 1.

193. *See* Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Facebook, Inc., No. 19-cv-2184, at 3, 15 (D.D.C. July 24, 2019) [hereinafter Facebook Order].

194. *Id.* at 8.

195. *Id.*

required to make quarterly compliance certifications to the FTC for which they can be personally civilly and criminally liable.[196]

Similarly, the combined FTC, CFPB, and multistate settlement with Equifax included more aggressive structural reforms than have been required by past FTC settlements.[197] For example, that settlement required that a written security program and evaluations be provided to the board annually.[198] The settlement also required Equifax to adopt specific policies and procedures and implement specific trainings including annual security awareness training and trainings for software developers.[199] In addition, the settlement required Equifax to establish a process for employees to submit concerns about the company's security practices.[200]

The Facebook and Equifax settlements came on the heels of several high-profile multistate settlements that included new structural reforms such as the Target and Uber settlements. Multistate settlements act as a catalyst for the FTC to pursue more demanding settlements. In fact, in the FTC's press release of the Facebook settlement, the FTC included a visual graphic showing the Facebook settlement to have the "[h]ighest [p]enalties in [p]rivacy [e]nforcement [a]ctions" as compared to prior multistate settlements.[201] The Facebook settlement was meant to set a standard for the industry in corporate governance and compliance programs.[202] The Facebook settlement is an indicator that the FTC will pursue more aggressive structural reform in future settlements, particularly in high-profile settlements.

Fourth, FTC settlements commonly require assessments by independent professionals and compliance reporting to ensure that the corporation has complied with the terms of the settlement.[203] These assessments generally occur biennially during the twenty-year term of the consent decree.[204] The auditors' biennial reports must be made available to the FTC.[205] Companies also agree to engage in record-keeping to facilitate the FTC's enforcement of the order.[206]

196. *Id.* at 10.

197. *See* Stipulated Order for Permanent Injunction and Monetary Judgment, Fed. Trade Comm'n v. Equifax, Inc., No. 1:19-cv-03297-TWT (July 23, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_order_signed_7-23-19.pdf [hereinafter Equifax Settlement].

198. *Id.* at 12–13.

199. *Id.* at 14.

200. *Id.* at 17.

201. *See* FTC Facebook Press Release, *supra* note 1.

202. *See* Ryan Tracy & Emily Glazer, *Landmark Facebook Settlement Still Working its Way Through Court*, WALL ST. J., Jan. 10, 2020.

203. *See, e.g.*, FTC Uber Settlement, *supra* note 186.

204. *See, e.g.*, *id.*

205. *See, e.g.*, *id.*

206. *See, e.g.*, *id.*

B. Elements of Multistate Settlements

Multistate and FTC data protection settlements share similar components, but there are notable differences in their settlement terms. Multistate settlements initially relied heavily on the FTC's established set of structural reform terms, especially in combined FTC/multistate settlements. But over time, AGs have charted new paths in their settlements by innovating terms that are distinct from the FTC's standard terms.

First, like FTC settlements, multistate settlements typically have injunctive provisions prohibiting misconduct that was the subject of the enforcement action.[207] For example, in the Uber multistate settlement, the company was barred from making misrepresentations about the extent to which Uber protected the personal information of riders and drivers.[208] These provisions also often require companies to comply with state laws such as consumer protection and data breach notification laws.[209] While settlements require companies to refrain from wrongdoing going forward, they typically do not require them to admit the allegations in the settlement.[210]

Second, unlike FTC settlements, multistate settlements typically require a civil penalty to be paid to the states in addition to potential restitution to consumers.[211] Penalties in multistate data protection settlements have ranged from $106,000[212] to $575 million.[213] Multistate settlements often settle in the multimillion-dollar range such as Google settling for $17 million in 2013,[214] Home Depot settling for 17.5 million in 2020,[215] Target settling for $18.5 million in 2017,[216] and Uber settling for $148 million in 2018.[217] In addition to

207. *See* Citron, *supra* note 23, at 761–62.

208. *See* Final Judgment and Consent Decree, Texas v. Uber Technologies, No. D-1-GN-18-005842, (Sept. 26, 2008), https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2018/Press/UBER%20Final%20Judgment%209%2026%2018.pdf [hereinafter Multistate Uber Settlement].

209. *See* Assurance of Voluntary Compliance, Investigation by Eric Schneiderman, Attorney General of the State of New York, of Target Corporation, No. 17-094 (May 2017), https://ag.ny.gov/sites/default/files/nyag_target_settlement.pdf [hereinafter Target Settlement].

210. *See, e.g.*, *id.* at 2.

211. *See* Citron, *supra* note 23, at 761–62. For a discussion on how penalties are allocated to states in multistate settlements, see Dishman, *supra* note 45, at 323.

212. *See* Assurance of Voluntary Compliance, Zappos.com, Inc. (Jan. 6, 2015) http://www.myfloridalegal.com/EC_Edoc.nsf/0/20761C17B266378485257DF20072A3B3/$file/Zappos.pdf [hereinafter Zappos Settlement].

213. The global Equifax settlement was $575 million; however, that amount includes consumer compensation and penalties to other regulators such as the CFPB and the states. *See* Equifax Press Release, *supra* note 28.

214. Brian Fung, *Why States Are the Big Winner in the $17 Million Google-Safari Settlement*, WASH. POST, Nov. 19, 2013.

215. *See* Morris, *supra* note 27.

216. *See AG Jepsen: Conn. Leads $18.5M Settlement with Target Corporation over 2013 Data Breach*, OFF. CONN. ATT'Y GEN. (May 23, 2017), https://portal.ct.gov/AG/Press-Releases-Archived/2017-Press-Releases/AG-Jepsen-Conn-Leads-185M-Settlement-with-Target-Corporation-over-2013-Data-Breach.

217. *See* Ohio AG Uber Press Release, *supra* note 29.

being allocated a portion of the penalties, leading states in multistate settlements may also receive attorneys' fees to compensate their offices for the resources expended in leading the action.[218] Multistate settlements are increasingly including public compensation for state residents who have been affected by the data breach.[219] For example, many states included a payment to Uber drivers as part of their state's share of the settlement.[220] Multistate settlements could be a greater source of restitution in the future if the FTC's ability to seek restitution is limited by pending Supreme Court cases.

Third, multistate settlements often incorporate the FTC's framework for structural reforms; however, they tend to be more customized to address the underlying conduct that brought rise to the actions. Like FTC settlements, multistate settlements often require corporations to establish reasonable "comprehensive information security programs."[221] They also typically require an employee to be responsible for the program, risk assessment, the implementation of safeguards, and testing and monitoring of those safeguards.[222] But multistate settlements differ from FTC settlements because they require companies to adopt more specific safeguards. FTC settlements generally include a broad provision that corporations must "design and implement . . . reasonable safeguards."[223] In contrast, multistate settlements often list the specific technological safeguards the corporation must adopt such as encryption, tokenization, multifactor authentication, and segmentation to address data breaches.[224] Multistate settlements also have provisions encouraging companies to develop or adopt new technologies to protect data and participate in pilot programs to test new security payment card technology.[225]

Multistate settlements have also required that companies adopt specific types of policies and procedures.[226] For example, the Uber multistate settlement

218. *See, e.g.*, Target Settlement, *supra* note 209, at 12. For a discussion of attorneys' fees in multistate actions see Dishman, *supra* note 45, at 323.

219. *See, e.g.*, Cox, *supra* note 137, at 2350–51.

220. *See, e.g.*, *AG Paxton Reaches $148 Million Settlement with Uber for Data Breach*, OFF. TEX. ATT'Y GEN. (Sept. 26, 2018), https://www.texasattorneygeneral.gov/news/releases/ag-paxton-reaches-148-million-settlement-uber-data-breach [hereinafter Texas AG Uber Press Release].

221. *See, e.g.*, Citron, *supra* note 23, at 781; Target Settlement, *supra* note 209, at 5.

222. *See, e.g.*, Target Settlement, *supra* note 209, at 6.

223. *See, e.g.*, Ashley Madison Settlement, *supra* note 189, at 5.

224. *See, e.g.*, Target Settlement, *supra* note 209, at 7–9; Assurance of Voluntary Compliance, Investigation by Letitia James, Attorney General of the State of New York, of The Home Depot Inc, No. 20-080 (Nov. 24, 2020), https://ag.ny.gov/sites/default/files/thd_avc_ny_final.pdf [hereinafter, Multistate Home Depot Settlement].

225. *See, e.g.*, Assurance of Voluntary Compliance, The TJX Companies, Inc. at 5–25 (June 23, 2009), https://www.nj.gov/oag/newsreleases09/pr20090623a-TJXCompaniesInc.pdf.

226. *Attorney General James Announces $1.5M Settlement with Retailer Neiman Marcus over Data Breach*, OFF. N.Y. ATT'Y GEN. (Jan. 8. 2019), https://ag.ny.gov/press-release/2019/attorney-general-james-announces-15m-settlement-retailer-neiman-marcus-over-data [hereinafter Neiman Marcus Settlement] (requiring written plans for software updates and replacement to protect personal data); Consent Judgment and Order, Arizona

required Uber to adopt a process to implement "privacy by design" principles in how Uber collects data about riders and drivers.[227] The Equifax multistate settlement required establishment of patch management policies and procedures.[228] And the Nationwide Insurance multistate settlement required policies surrounding common vulnerabilities and exposures (CVEs).[229] In addition to requiring specific policies and procedures, multistate settlements have also required regular review of specific policies.[230]

Multistate settlements have specifically mandated employee training relating to the underlying data problem that gave rise to the enforcement action.[231] For example, TD Bank and a multistate group agreed to a settlement after some of TD Bank's unencrypted backup tapes storing personal information were lost during their transportation.[232] The multistate settlement required TD Bank to conduct employee training on the proper handling of backup tapes.[233] The Google multistate settlement required the company to provide specific certifications for employees and hold an annual privacy week to train employees about privacy protection.[234] Furthermore, the Google multistate settlement required legal counsel to undergo privacy training.[235] The Uber multistate settlement required employees to participate in ongoing training on handling personal information in addition to annual training on Uber's Code of Conduct.[236] The Home Depot settlement required annual security awareness and privacy training.[237] In contrast, FTC settlements

et al. v. Medical Informatics Engineering, No. 3:18-cv-969-RLM-MGG (N.D. Ind. May 23, 2019) [hereinafter Medical Informatics Engineering Settlement] (requiring policies and procedures for system logs, passwords, and security incidents).

227. Multistate Uber Settlement, *supra* note 208, at 10.

228. Equifax Settlement, *supra* note 197, at 14.

229. Assurance of Voluntary Compliance, Nationwide Mutual Insurance Company and Allied Property & Casualty Insurance Company (July 25, 2017), https://ag.ny.gov/sites/default/files/nationwide-aod.pdf [hereinafter Nationwide Insurance Settlement].

230. *See* Assurance of Voluntary Compliance, TD Bank, N.A. (Oct. 3, 2014), https://portal.ct.gov/-/media/AG/Press_Releases/2014/20141016OAGCDPTDBankSettlementpdf.pdf?la=en [hereinafter TD Bank Settlement] (requiring biennial review of policies and procedures related to the transportation of personal information); Assurance of Voluntary Compliance, Adobe Systems Inc. (Nov. 11, 2016) https://www.ohioattorneygeneral.gov/Files/Briefing-Room/News-Releases/Consumer-Protection/2016-11-10-Adobe-AVC-Final.aspx [hereinafter Adobe Settlement] (requiring twice annual review of security policies).

231. *See, e.g.*, Equifax Settlement, *supra* note 197, at 16; Multistate Uber Settlement, *supra* note 208, at 7.

232. TD Bank Settlement, *supra* note 230.

233. *Id.* at 4–5.

234. Assurance of Voluntary Compliance, Google Inc. (Mar. 11, 2013), https://portal.ct.gov/-/media/AG/Press_Releases/2013/20130312GoogleAVCpdf.pdf?la=en [hereinafter Google Street View Settlement].

235. *Id.*

236. Multistate Uber Settlement, *supra* note 208, at 7.

237. Multistate Home Depot Settlement, *supra* note 224, at 5.

generally include training as a category that corporations consider as part of their risk assessment.[238]

Multistate settlements have required increased information flow about data protection to the C-suite and the board of directors. FTC settlements have typically only required that the board of directors and executives receive a copy of the consent decree.[239] In contrast, some multistate settlements require that information security executives regularly report to the CEO and board.[240] For example, the multistate settlement with Premera Blue Cross requires that the chief information security officer provide a report to the board of directors annually, to the CEO every two months, and the chief information officer twice a month.[241] The Uber multistate settlement requires that the security executive report quarterly to the CEO, chief legal officer, and board regarding data security incidents.[242] The Home Depot settlement requires that the job description for the new "Chief Information Security Officer" include responsibilities for advising the CEO and board of directors about the company's security risks and posture.[243]

Multistate settlements have required companies to provide means for employees to report concerns about information security and any other misconduct. In the Uber multistate settlement, Uber had to set up a hotline for employees to report misconduct.[244] Reports of misconduct from the hotline are reported to the board of directors or a board committee at each scheduled meeting.[245] The Equifax settlement required that the company establish a process for employees to report concerns about information security.[246]

Multistate settlements also have distinctive provisions relating to consumer education. Multistate settlements have required corporations to provide consumer education relating to the enforcement action. For example, Google entered into two different multistate settlements that included specific requirements for consumer education. In one instance, the Google Street View car inadvertently collected personal information from people's wireless networks as the car was capturing images for its Google Maps application (app).[247] In the settlement, Google was required to launch a public campaign to

238. *See, e.g.*, FTC Uber Settlement, *supra* note 186, at 3.

239. *See, e.g.*, Ashley Madison Settlement, *supra* note 189, at 11.

240. *See, e.g.*, Multistate Uber Settlement, *supra* note 208; Target Settlement, *supra* note 209; Premera Blue Cross Settlement, *supra* note 153.

241. *See* Premera Blue Cross Settlement, *supra* note 153, at 10.

242. Multistate Uber Settlement, *supra* note 208, at 9.

243. Multistate Home Depot Settlement, *supra* note 227, at 5.

244. *Id.* at 10.

245. *Id.*

246. Equifax Settlement, *supra* note 197, at 16.

247. *See* Eyder Peralta, *Google Will Pay $7 Million to Settle View Data Capturing Case*, NPR (Mar. 12, 2013), NPR.org, https://www.npr.org/sections/thetwo-way/2013/03/12/174117502/google-will-pay-7-million-to-settle-street-view-data-capturing-case.

teach consumers about securing wireless networks that included YouTube videos and blog postings.[248] In another instance, Google used cookies to bypass privacy settings that were established by consumers.[249] In that instance the settlement required that Google create a webpage explaining cookies to consumers.[250]

Multistate settlements have mandated that corporations engage in data breach planning to protect consumers in the future. Under the terms of the settlements, corporations must create response plans for future data breaches including consumer notification. For example, the Uber multistate settlement sets forth several specific provisions for a data breach response and notification plan.[251] The Uber data breach response plan requires the company to identify data security incidents, describe each individual's responsibilities under the plan, and regularly test and review the plan.[252] It also requires that once Uber determines there is a data security breach, a licensed attorney must evaluate whether consumer notification is required, and the attorney's opinion must be communicated in writing to Uber's security executive.[253] Data breach notification plans may also include a requirement to notify AGs of data breaches that involve their state residents.[254]

Fourth, multistate settlements contain provisions for third-party assessments and compliance reporting. FTC settlements also require third-party assessments and monitoring. However, the term of multistate settlements tends to be much shorter in duration than FTC settlements. Multistate settlements typically have fewer reporting requirements and less oversight. When there is a joint FTC and multistate settlement, the term of the settlement is the FTC's typical twenty-year term with third-party assessments occurring biannually over the term.[255] But when the settlement just includes states, the term is significantly shorter. The term for multistate settlements varies from two years[256] to ten years.[257] The most common duration of multistate settlements is five years.[258] Some multistate settlements require annual assessment for the term of settlement, but others only require a single independent assessment.[259] The

248. Google Street View Settlement, *supra* note 234, at 5–6.

249. *See* Claire Cain Miller, *Google to Pay $17 Million to Settle Privacy Case*, N.Y TIMES (Nov. 19, 2013), https://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html.

250. Assurance of Voluntary Compliance, Google Inc. (Nov. 13, 2013), https://portal.ct.gov/-/media/AG/Press_Releases/2013/20131118GoogleSafariAVCExecutedpdf.pdf?la=en [hereinafter Google Safari Settlement].

251. *See* Multistate Uber Settlement, *supra* note 208.

252. *Id.*

253. *Id.*

254. *See, e.g.*, Adobe Settlement, *supra* note 230, ¶ 22; Multistate Uber Settlement, *supra* note 208, at 8.

255. *See, e.g.*, Ashley Madison Settlement, *supra* note 189.

256. *See* Zappos Settlement, *supra* note 212 (two years).

257. *See* Multistate Uber Settlement, *supra* note 208 (ten years).

258. *See, e.g.*, Target Settlement, *supra* note 209.

259. *See* Medical Informatics Engineering Settlement, *supra* note 226; Adobe Settlement, *supra* note 230.

difference in the length of term between FTC and multistate settlements may be due to the fact that states can collect civil penalties in the first instance, whereas the FTC can only collect civil penalties when an existing consent decree has been violated. Because states can collect penalties in the first instance, there is less of a need to have a lengthy term to monitor compliance with the settlement in order to collect penalties.

Relatedly, ongoing monitoring is generally less onerous in multistate settlements than FTC settlements. Corporations must submit compliance certificates to a group of AGs or a single leading AG.[260] AGs have the right to request documentation to assess the company's compliance with the settlement and companies are required to keep records.[261] However, because multistate enforcement actions are made up of an ad hoc group of states, there is no ongoing structure in place to monitor compliance with the settlement. In order to enforce a multistate settlement, each AG would have to bring action in their own state court.[262] Moreover, some multistate settlements require that AGs provide notice to corporations and give them an opportunity to respond prior to instigating an enforcement action based on violation of the settlement agreement.[263] This means that each AG participating in the settlement is responsible for monitoring and enforcing the settlement. Given the many demands on generalist AG offices, AGs have less capacity to monitor multistate settlements than a specialist agency like the FTC. The FTC has the permanence, resources, and capacity to engage in long-term monitoring while ad hoc groups of states in individual actions do not have the same long-term monitoring capacity.

The difference in approaches in FTC and multistate settlements can be encapsulated by contrasting the FTC and multistate settlements with Uber. The FTC and a multistate group, including all fifty states and the District of Columbia, settled separately with Uber.[264] Both settlements arose from the same data breach incident at Uber. Furthermore, the settlements occurred within one month of each other, with the multistate settlement being entered prior to the FTC settlement.[265]

The FTC Uber settlement was very similar to the FTC's past data protection settlements with other companies. The settlement included the FTC's standard structural reforms including the requirement to establish a "comprehensive privacy program" with a designated employee to oversee the

260. *See, e.g.*, Adobe Settlement, *supra* note 230 (assessment provided to the Connecticut AG); Multistate Uber Settlement, *supra* note 208 (assessment provided to the California AG).

261. *See* Nationwide Insurance Settlement, *supra* note 229.

262. *See* Citron, *supra* note 23, at 761.

263. *See, e.g.*, Premera Blue Cross Settlement, *supra* note 153, at 22–23.

264. Lydia F de la Torre, *The Uber Breach Story: On How Security Woes Can Lead to a Criminal Complaint*, MEDIUM (May 13, 2019), https://medium.com/golden-data/case-study-uber-technologies-inc-data-breach-7261484d6471.

265. *See* FTC Uber Settlement, *supra* note 186, at 9; Multistate Uber Settlement, *supra* note 208, at 1.

program.[266] Like other settlements, Uber was required to engage in risk assessment, design reasonable controls based on its risk assessment, and evaluate its privacy programs based on its testing and monitoring.[267] The FTC Uber settlement also included biennial privacy assessments by an independent third party for the twenty-year term of the settlement.[268]

The multistate Uber settlement incorporated standard FTC settlement provisions but included more specific settlement terms in addition to innovating new terms relating to Uber's corporate integrity program. The multistate settlement incorporated the FTC's framework by requiring a "comprehensive information security program," risk assessment, reasonable safeguards, and testing and monitoring.[269] It also required independent biannual third-party assessment although for a shorter period than the FTC settlement.[270] But the multistate settlement deviated from the standard FTC settlement by including more specific provisions such as requiring the adoption of specific safeguards, including password and encryption policies and mandating ongoing training on proper handling of personal information of Uber drivers and riders.[271]

The multistate settlement required distinct corporate governance terms that extended well beyond data protection.[272] The multistate settlement focused on reporting and on information flow relating to any misconduct at Uber, not just reporting on data incidents. The settlement required Uber to set up a hotline for employees to report misconduct.[273] It also specifically addressed information about misconduct to flow to the Uber C-Suite and Board of Directors. An executive or officer is required to report at each meeting of the Board of Directors complaints, violations of policies, or reports from the hotline.[274] It also required Uber's Security Executive to regularly advise the CEO or Chief Legal Officer of the security posture at Uber.[275]

The FTC and multistate settlements differed on their provisions related to data breach notification. The FTC requires Uber to provide the FTC with reports related to data violations. These "[c]overed [i]ncident [r]eports" must detail the data incident, the remediation taken, and notice provided to consumers.[276] The Uber multistate settlement has more expansive terms with respect to data breaches, including requirements to prospectively plan for future

266. FTC Uber Settlement, *supra* note 186, at 3.
267. *Id.*
268. *Id.*
269. Multistate Uber Settlement, *supra* note 208, at 6.
270. *Id.* at 7.
271. *Id.* at 5–7.
272. *Id.* at 10.
273. *Id.*
274. *Id.*
275. *Id.*
276. FTC Uber Settlement, *supra* note 186, at 4–5.

data breaches. The multistate settlement requires the adoption of a "comprehensive Incident Response and Data Breach Notification Plan."[277] Under the multistate settlement, Uber must adopt a plan to identify future data breach incidents and have people in place to fulfill responsibilities under the plan.[278] Specifically, the plan requires an attorney to determine whether breach notifications are required and regular reporting to the CEO, Chief Legal Officer, and the Board about data security incidents.[279]

There was also a dramatic difference in the amount of penalties in the FTC and multistate settlements. The FTC Uber settlement was a $0 settlement, with no penalties for the FTC or consumer restitution.[280] However, the multistate settlement included a record-breaking $148 million.[281] Several participating states included payments to Uber drivers as part of its allocation of the multistate settlement.[282]

Although multistate settlements have relied on the FTC's traditional structural reforms, they have also charted new paths in data protection enforcement by innovating new settlement terms. They have demanded more specific and customized safeguards, policy changes, and structural reforms to increase transparency and accountability.

C. Borrowing in Data Protection Enforcement

The FTC and AGs each have comparative advantages and disadvantages in data enforcement. These advantages and disadvantages are an extension of their enforcement authority and institutional characteristics. Their different approaches to settlement reflect their different enforcement strengths and weaknesses. The FTC and AGs can borrow from each other's enforcement strengths to augment their abilities to regulate data practices through settlement.

The FTC has strengths and weaknesses as a data enforcer. Many of its strengths are derived from its institutional characteristics as a federal agency. As a federal agency, the FTC has specialized expertise, capacity, and permanence. The FTC has established expertise in data practices. It was one of the first agencies to enforce data practices[283] and has grown to be the primary data enforcement agency. It has developed a precedent for data enforcement settlements. This consistent approach to settlement terms provides uniformity and predictability for regulated entities. The FTC also has dedicated staff and

277. Multistate Uber Settlement, *supra* note 208, at 8.

278. *Id.* at 9.

279. *Id.*

280. *See* FTC Uber Settlement, *supra* note 186.

281. Multistate Uber Settlement, *supra* note 208, at 11.

282. *See* Texas AG Uber Press Release, *supra* note 220.

283. Chris Jay Hoofnagle et al., *The FTC Can Rise to the Privacy Challenge, but Not Without Help From Congress*, BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress.

resources that allow the agency to engage in ongoing monitoring and oversee compliance with consent decrees. As an independent agency, the FTC is more politically insulated, which allows it to rely on its expertise to make difficult trade-offs between consumers' interests and promoting economic development and innovation.[284] At the same time, the FTC faces enforcement challenges, particularly related to its enforcement authority and rulemaking abilities. The FTC is in an awkward position because it must argue to litigants that its enforcement authority is clear, but at the same time petition Congress to grant it the very authority it claims to already have in litigation.

The FTC's strengths as a data enforcer are reflected in its settlements. The agency's permanence and stability are reflected in the long term of settlements because the agency has the institutional capacity to monitor them over a twenty-year period. The uniformity of its settlement terms and structural reforms is also mirrored in the agency's stability and desire to create consistent precedent. Broader, more generalized terms requiring reasonability in FTC settlements may also be a function of the FTC's institutional permanence because the FTC has the ongoing ability to define what is "reasonable" and provide guidance based on current technology and best practices.

The FTC's uncertain authority is reflected in its settlement terms. The FTC's structural reforms defer to the company to establish a "reasonable comprehensive" security or privacy program and make policy changes based on their own risk assessment, instead of requiring more specific data safeguards. The FTC may have adopted more generalized, deferential, and consistent settlement terms in an effort to stave off challenges to its authority to enforce data practices. If the FTC were to require more specific and demanding structural reforms, targets may be more likely to challenge the FTC's authority. Because of the hurdles the FTC faces to engage in formal rulemaking, it is particularly important that the agency maintain its enforcement authority via settlement since this is the primary means the FTC uses to regulate data practices.

AGs have strengths in data protection enforcement such as their strong data enforcement authority. States' authority to enforce their UDAP laws has not been challenged in litigation like the FTC's authority. State legislatures have passed additional data protection laws supporting AG's' enforcement authority, including data breach notification laws and comprehensive data protection statutes. Furthermore, enforcement authority has been delegated to AGs under several federal statutes. In addition to their strong enforcement powers, AGs are nimble, entrepreneurial data enforcers. They are not as bound by precedent in settlement terms and are more likely to experiment with new terms. AGs are also democratically elected officials. As a result, AGs are more likely to be

284. *Id.*

responsive to consumers who are impacted by data breaches and privacy violations.

AGs enforcement strengths are reflected in the terms of multistate settlements. AGs' strong enforcement authority allows them to be more demanding, specific, and creative with structural reform provisions. As a result, multistate settlements have greater variance in terms among settlements. Multistate settlements tend to be more customized to the underlying data violations than their FTC counterparts. The ability to seek civil penalties in the first instances also removes the need for longer term settlements and ongoing compliance monitoring. Thus, multistate settlements tend to have shorter terms and have less onerous requirements for third-party assessment and ongoing monitoring. AGs' democratic accountability may also account for terms in multistate settlements that relate to consumer education, such as requirements that companies create videos or blog posts to better educate consumers about data risks.

Multistate data enforcement also has weaknesses that are reflected in their settlements. Multistate groups are ad hoc groups brought together for the purpose of pursing an individual enforcement action. Multistate enforcement lacks the permanence of a federal agency. As a result, it is more difficult for states to engage in ongoing compliance monitoring in settlements. Reporting requirements in multistate settlements mandate that assessments be submitted to leading AGs. There is no institution that oversees and enforces the settlement. Rather, the onus is on each individual AG to enforce the settlement agreement. The shorter terms of settlements and less onerous third-party assessments and compliance monitoring in multistate settlements reflects the lack of institutional permanence in multistate enforcement.

The FTC and AGs have generally had a cooperative enforcement relationship and borrowed from one another's data enforcement strengths. AGs have borrowed the FTC's institutional permanence and capacity for ongoing compliance monitoring of data protection settlements. Multistate groups rely on the FTC's monitoring ability when they join settlements with the FTC and the FTC is primarily responsible for ongoing settlement monitoring.[285] This is reflected in the fact that combined FTC/multistate settlements have the longer twenty-year term and include the FTC's standard third-party assessment and ongoing monitoring terms. Multistate settlements have also piggybacked on the FTC's capacity to supervise settlements by incorporating the monitoring requirements from prior FTC settlements into later multistate settlements. For example, a Google multistate settlement referred to a prior FTC settlement with Google and required Google to provide

285. *See* Equifax Settlement, *supra* note 197, at 61–62.

the assessments from the FTC settlements to the multistate group going forward for the term of the FTC consent decree.[286]

Multistate settlements have also borrowed from the FTC's established precedent of consistent settlement reforms. Multistate settlements have relied on the FTC's structural reforms as a framework. When they do so, they borrow the legitimacy for the terms in their settlements based on FTC precedent. However, multistate settlements have adapted that framework with more specific or customized terms. Multistate settlements have been able to borrow the FTC's precedent and use it as a foundation to innovate new structural reform terms.

The FTC can likewise borrow from innovative terms in multistate settlements. Multistate settlements can spur the FTC to demand more aggressive structural reforms. In recent high-profile FTC settlements, the FTC has deviated from its standard structural reforms and required more demanding reforms. For example, the FTC's recent settlements with Facebook and Equifax included new, more demanding and specific structural reforms. These settlements incorporated principles from previous multistate settlements such as requirements for increasing reporting to the board and executives about data issues and specific employee training requirements.[287] Multistate settlements can create precedent for FTC settlements to borrow more aggressive structural reforms in the future. Once parties have agreed to terms with multistate groups, the FTC may be on stronger footing to make the same demands or rely on the multistate settlement to institute those terms in future settlements.

The FTC can also borrow states' stronger data enforcement authority.[288] By combining with states, the FTC can rely on state's enforcement authority to include provisions that the FTC may not have the authority to require on its own. For example, combined FTC/multistate settlements include data breach notification terms. The FTC can rely on state data notification laws to provide the authority for those terms because there is no federal law requiring such notifications. Companies may be less likely to challenge combined FTC/ multistate settlements when the FTC is partnering with states that have stronger enforcement authority.

The Uber FTC and multistate settlements provide an example of how borrowing can work between the FTC and multistate groups. The multistate Uber settlement was able to rely on the FTC's standard framework for structural reforms, while adopting more specific requirements and innovating new terms. The FTC could rely on states' data breach notification statutes to implement terms about data breach notification, since there is no federal data

286. Google Street View Settlement, *supra* note 234, at 5.

287. *Id.* at 16 (requiring "[t]raining for software developers relating to secure software development principles").

288. *See* Gregory James Evans, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Beaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 214 (2015).

breach notification law, but only state law requiring notifications of consumers. In fact, terms requiring data breach or "covered incident" reporting are a relatively new addition to FTC settlements, including the Facebook settlement, and the inclusion of these terms could be a result of relying on multistate innovation and state law.[289]

Furthermore, the states and the FTC can work together to expand the FTC's enforcement authority. The "FTC cannot directly enforce state laws," but if a company violates state law that deceives consumers, the "FTC can enforce its Section 5 prohibition against [the company's] deceptive practices."[290] If states require that companies make certain data representations and those representations turn out to be untrue, the FTC may bring an enforcement action by claiming that the violation constitutes a deceptive practice under Section 5.[291] In this manner, the FTC can expand its enforcement authority by relying on state data protection laws.[292]

The FTC and AGs have comparative advantages and disadvantages in data enforcement. By borrowing from one another, they can compensate for their weaknesses. At the same time, borrowing enables enforcers to more potently regulate by settlement, rather than pursue other forms of regulation, such as rulemaking or legislation.

III. REGULATION BY SETTLEMENT

FTC and multistate settlements are vehicles for nationally regulating data practices. Courts and commentators have raised concerns about regulation through enforcement settlements in general and specifically in the context of FTC data enforcement settlements.[293] However, these concerns have not been raised with respect to multistate settlements even though unique attributes of multistate enforcement exacerbate previously identified concerns about regulation by settlement and raise entirely new ones.

A. Regulation by FTC Settlement

Regulation by settlement bypasses traditional checks on policymaking that are more participatory and transparent, such as the legislative process, rulemaking, and judicial review.[294] Circumventing these checks consolidates significant discretion and policymaking power in enforcers.[295] Agency enforcers

289. *See, e.g.*, Facebook Order, *supra* note 193.

290. Evans, *supra* note 288, at 213 (footnote omitted).

291. *Id.* at 218–19.

292. *Id.* at 214–18.

293. *See, e.g.*, Turk, *supra* note 37, at 261–63; Garrett, *supra* note 37, at 1484.

294. *See* Davidoff & Zaring, *supra* note 40, at 468; Turk, *supra* note 37, at 324.

295. Garrett, *supra* note 37, at 1485.

who are in career positions are not directly democratically accountable. And as an independent agency, the FTC is particularly isolated from democratic accountability and oversight.[296]

The legislative process is more transparent and participatory than regulation by settlement.[297] Members of Congress are elected and democratically accountable to their electorates. Bills are publicly available for review and formal legislative proceedings are open to the public. The legislative process invites participation by relevant stakeholders making the process more transparent and participatory.

Agency rulemaking is also more participatory and transparent than regulation by settlement.[298] Notice and comment procedures allow the public and stakeholders to comment on proposed regulations. Comments are taken into consideration prior to the finalization of a regulation and are available for public review. Final regulations are published in the Code of Federal Regulations (CFR) and are accessible to the public and regulated entities.

In contrast to the legislative and rulemaking process, regulation by settlement excludes stakeholders that are not the subject of the enforcement action. Stakeholders are excluded from the settlement process even though the policies developed in settlements are meant to be communicated and applied in the future to the broader industry.[299] This approach excludes the information and arguments that stakeholders can provide to define the competing interests involved and educate the agency about the tradeoffs involved policymaking.[300] It is also not a transparent form of regulation because policymaking discussions are contained within the negotiation of the parties to the enforcement action.

FTC procedures require a notice and comment period for proposed settlements. However, this procedure is not as transparent and participatory as the notice and comment process in formal rulemaking. Notice and comment in rulemaking may result in an agency changing the proposed regulation. In the settlement context, however, there is generally little, if any, change made to settlements based on public comment. This may be because it is difficult to change the terms of a negotiated agreement between parties.

In addition to bypassing democratic checks, regulation by settlement often evades judicial review.[301] Courts play an important role in formal adjudication by agencies such as in cases that are litigated before an administrative law judge or in federal district courts. But in an informal disposition where the parties settle, courts provide limited oversight. Of the FTC's many settled data

296. William E. Kovacic & Marc Winerman, *The Federal Trade Commission as an Independent Agency: Autonomy, Legitimacy, and Effectiveness*, 100 IOWA L. REV. 2085, 2087 (2015).

297. *See* Turk, *supra* note 37, at 295.

298. *See* Bressman, *supra* note 37, at 541–42.

299. *See* Stegmaier & Bartnick, *supra* note 14, at 714.

300. *See* Bressman, *supra* note 37, at 542.

301. *See* Turk, *supra* note 37, at 262; Davidoff & Zaring, *supra* note 40, at 468.

protection cases, there are only a few cases where parties have litigated instead of settling prior to litigation with the FTC.[302] While courts may approve consent decrees, courts are generally deferential to agencies and provide little meaningful oversight.[303] Limited court oversight consolidates power in the FTC to regulate wide swaths of the economy through enforcement actions. This raises concerns about separation of powers because it consolidates the roles of rulemaking, enforcement, and adjudication into one branch of government.[304]

Overly broad regulation may result from the settlement process and the incentives of the parties to the settlement. The process of settlement is a poor vehicle for regulation because it is a negotiated outcome for parties arising from a specific set of facts. The incentives of settling parties are not necessarily well-aligned with the socially beneficial development of the law.[305] In order to best marshal resources, the FTC will often take easy cases where the target will settle, rather than litigate.[306] Easy targets may make bad regulation as it may result in overly broad policies that do not consider the nuances that occur in harder cases. At the same time, regulation by settlement may "approach broad policy questions from a narrow perspective—only as necessary to decide a case—which decreases the comprehensiveness of the resulting rule."[307] When settlements convey regulation narrowly by resolving a specific case, it "decreases predictability" and planning opportunities for companies trying to develop their future practices.[308]

Targeted companies are not well-suited to consider the balancing of interests in policymaking, instead preferring to resolve the action as quickly and inexpensively as possible. They are not incentivized to vigorously litigate with the FTC because there are no financial penalties in most settlements. Thus, companies may agree to overly broad or vague settlement terms simply to avoid the financial and reputational costs of drawn-out negotiation and litigation.

Regulation by settlement has been criticized as being so vague that regulated entities lack fair notice of what behavior complies with the law.[309] Regulated entities are entitled to fair notice of whether or not their actions comply with the law.[310] Agencies have not provided fair notice if a company,

302. *See, e.g.*, F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d. Cir. 2015); LabMD, Inc. v. F.T.C., 894 F.3d 1221 (11th Cir. 2018).

303. Garrett, *supra* note 37, at 1485; *see* Hillary A. Sale, *Judges Who Settle*, 89 WASH. UNIV. L. REV. 377, 408 (2011).

304. *See* Garrett, *supra* note 37, at 1487.

305. Hurwitz, *supra* note 42, at 983.

306. *See* Solove & Hartzog, *supra* note 10, at 613.

307. Bressman, *supra* note 37, at 542.

308. *Id.*

309. *See generally* Geoffrey A. Manne & Kristin Stout, *When "Reasonable" Isn't: The FTC's Standardless Data Security Standard*, 15 J. L. ECON. & POL'Y 67 (2019).

310. Stegmaier & Bartnick, *supra* note 14, at 677.

"acting in good faith cannot identify with 'ascertainable certainty'" the agency's standards for compliance.[311]

Regulated entities can challenge a "legal rule that imposes penalties" but "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement."[312] Fair notice raises concerns as to whether regulators are meeting basic constitutional due process requirements.[313] Due process concerns are heightened "when an agency has not promulgated a formal rule and, instead, uses its enforcement conduct to define the contours of its broad discretion."[314]

The FTC has been criticized for failing to provide fair notice in enforcement actions pursuant to its unfairness authority under Section 5. For example, the FTC has brought enforcement actions based on data breaches arguing that companies' data protections were so unreasonable as to make them unfair.[315] FTC settlements typically require that companies establish a "comprehensive information security program."[316] Both commentators and regulated entities have criticized this vague standard as not providing companies sufficient notice of what practices a company must adopt to avoid violating Section 5.[317]

Other concerns have been raised about the ambiguity of FTC settlements. For example, it is difficult to discern from the settlements which facts were important to the FTC's unfairness determination and how the FTC weighted those facts. Importantly, the FTC settlements do not address how the target's size or the scale of the data breach plays a role in the company's failure to implement any specific data security safeguard. Rather, the relevant facts tend to be "lumped together" in complaints and settlements.[318] Complaints and settlements may also differ in "identifying noncomplying practices and imposing data-security safeguards."[319] This ambiguity leaves non-parties to guess whether they should follow the complaint, consent decree, or both in order not to run afoul of Section 5 and "result in a prohibited unfair practice."[320] It is also difficult for non-parties to determine what safeguards are

311. Stegmaier & Bartnick, *supra* note 14, at 677.

312. Hurwitz, *supra* note 42, at 1002.

313. *Id.* (citations omitted).

314. Stegmaier & Bartnick, *supra* note 14, at 677.

315. *See, e.g.*, F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 241–42 (3d Cir. 2015).

316. *Id.* at 255.

317. *See, e.g.*, *id.* at 255 ("[The regulated entity] argues . . . it lacked notice of what specific cybersecurity practices are necessary to avoid liability."); Equifax Settlement, *supra* note 197, at 12 (ordering Equifax to "establish and implement False . . . a comprehensive information security program"); Manne & Stout, *supra* note 309, 74–76 (arguing that "even the most comprehensive industry standards False . . . is inconsistent with the set of 'reasonable' practices that might be derived from the FTC's consent orders").

318. Manne & Stout, *supra* note 309, at 75.

319. Stegmaier & Bartnick, *supra* note 14, at 693–94.

320. *Id.*

required to be in compliance with Section 5 and what safeguards are simply advisable best practices.[321]

Ambiguity in regulation unnecessarily burdens companies and ultimately consumers.[322] On the one hand, companies, faced with vague regulation, may over-invest in unnecessary data security, instead of spending resources investing in employees, products, and services.[323] On the other hand, ambiguity can lead to easy evasion of data regulations, leaving consumers with less data security than they might receive if there were clearer standards.[324] Furthermore, vagueness in regulation can be particularly detrimental to smaller companies that cannot afford to overinvest in data security.[325] Smaller companies, including technology start-ups, also face greater risks because they lack the resources to pay penalties or defend enforcement actions.[326] In fact, LabMd, a small laboratory company, became defunct due to the resources it expended litigating the FTC.[327]

The lack of predictability from this form of regulation is exacerbated by lack of accessibility. Regulation by settlement "announces policy in the form of an order rather than codifying it in the Federal Register."[328] The FTC keeps complaints and consent decrees on its website. A regulated entity must wade through many decrees and complaints to establish a pattern of regulation. The FTC is rarely the primary regulator of most companies, so companies do not often look first to the FTC for regulatory guidance. Larger companies are likely to be better informed because they can afford a privacy lawyer who knows to consult the FTC website and pour over FTC complaints and consent decrees. However, smaller companies are unlikely to have the funds available to hire specialized legal professionals to search through the FTC's online archives.

There are many problems with regulating by settlements for federal agencies like the FTC. While scholars have considered these problems in the context of data protection regulation and the FTC, they have not considered these concerns in light of the rise of multistate enforcement settlements.

B. Regulation by Multistate Settlement

Multistate settlements raise the same concerns as federal agencies regulating by settlement. However, the unique attributes of multistate enforcement

321. Stegmaier & Bartnick, *supra* note 14, at 693–94.

322. *Id.* at 710–11.

323. *Id.* at 711.

324. *Id.*

325. *Id.*

326. *Id.*

327. *See* Mike Scarcella, *FTC Ordered to Pay $843K in Legal Fees, Costs After Losing Privacy Cases*, LAW.COM (Dec. 26, 2019), https://www.law.com/nationallawjournal/2019/12/26/ftc-is-ordered-to-pay-843k-in-legal-fees-costs-after-losing-privacy-case.

328. Bressman, *supra* note 37, at 532.

exacerbate those concerns and raise entirely new ones. Like FTC settlements, multistate settlements are a form of regulation that sidestep more transparent, accountable, and participatory forms of policymaking. Multistate settlements similarly suffer from vagueness and lack of predictability. To compound these problems, there are fewer procedural protections in multistate settlements than FTC settlements.

Multistate settlements bypass traditional checks in the policymaking process,[329] but they do so in ways that are even less participatory and transparent than their FTC counterparts. Multistate settlements are negotiated behind closed doors with little involvement from outside stakeholders.[330] Even though many states may participate in a multistate action, only a few leading AGs actually negotiate the settlement.[331] The few leading AGs who negotiate the settlement are democratically accountable to their own state electorates but not to the broader group of stakeholders who are affected by the settlements.

It could be argued that there is more democratic accountability in regulation by multistate settlement because individual AGs are elected by their state residents. While individual AGs are more directly democratically accountable than federal agency enforcers, only a small group of AGs usually lead multistate actions, and they are only accountable to their own state residents.[332] That means that a small number of AGs are making national policy through settlements but are only accountable to their own states.[333] Multistate settlements thus result in national policymaking that excludes important stakeholders who may not be represented by voters from a few states.

This limited democratic accountability raises a new concern about regulating by multistate settlement. AGs may not be well-positioned to craft nationally regarding policies when they are only democratically accountable to their own state residents.[334] The policy trade-offs that an AG may consider are likely to be different than a federal agency because AGs represent a more limited constituency. AGs are incentivized to prioritize their state residents over national interests if the two conflict. For example, an AG may prioritize strict consumer data protection because it benefits her state electorate, but these protections may place considerable burdens on the national economy and innovation. In contrast, a federal agency may be better suited to consider the national ramifications of policies because they are not democratically accountable to a single state.

329. *See* Gifford, *supra* note 31, at 961.

330. NOLETTE, *supra* note 32, at 26.

331. *Id.* at 26; Provost, *supra* note 33, at 6–8; Dishman, *supra* note 45, at 307.

332. *See* Dishman, *supra* note 45, at 306–07.

333. *Id.* at 342–43.

334. *See* Rose, *supra* note 53, at 1372.

Ambitious AGs seeking re-election or election to a higher office may also prioritize making splashy headlines over creating nationally cohesive policy.[335] Thus, AGs may seek large settlement amounts that generate publicity instead of developing meaningful structural corporate reforms that may not resonate as well with voters. Indeed, the headlines of press releases for multistate settlements typically include the global amount of the settlement, while structural reforms, if mentioned at all, are usually relegated to lower in the body of the press release.[336] If AGs do not think that structural reform resonates with voters, it may not be a priority for AGs to carefully craft those terms.

There are few procedural protections in place to increase transparency and participation in the multistate settlement process. Unlike FTC settlements that allow for a notice and comment period before a settlement is finalized, multistate settlements lack the same process for comment by outside stakeholders.[337] FTC settlements additionally require majority approval by the FTC Commissioners.[338] Multistate settlements lack the review provided by the Commissioners.

Multistate settlements are also particularly vulnerable to the criticism that they evade judicial review. State courts play an extremely limited role with respect to multistate settlements. Some states' statutes do not require court approval for settlements.[339] In states that require court approvals, courts are deferential, often acting as a rubber stamp without providing meaningful review.[340] Even when multistate actions are in federal court, in many instances, courts are deferential, and there is little meaningful review of multistate settlements.[341]

AGs may lack the institutional capacity to be effective regulators, particularly in the area of data protection. AGs are "generalist enforcers" with limited resources that may lack the capacity to be national policymakers, especially in areas that require technological expertise.[342] That being said, AGs have made tremendous strides in increasing their institutional sophistication to pursue multistate actions and access technical expertise.[343]

335. *See* Lemos, *supra* note 49, at 515 n.123.

336. *See, e.g.*, Texas AG Uber Press Release, *supra* note 220.

337. *See Overview of FTC Authority*, *supra* note 47.

338. *See, e.g.*, FTC Facebook Press Release, *supra* note 1 (reporting that the Commission vote on the compliant and stipulated order was 3-2).

339. Rather, state courts may only require that the settlement be filed in state court. *See* Dishman, *supra* note 45, at 347.

340. *See* Dishman, *supra* note 45, at 347; *see generally* Lemos, *supra* note 49, at 537; Garrett, *supra* note 37, at 1542.

341. Multistate actions based on federal law are required to be filed in federal district court. *See* Lemos, *supra* note 150, at 757.

342. *See* Dishman, *supra* note 34, at 435.

343. *See* Citron, *supra* note 23, at 755; NOLETTE, *supra* note 32, at 213.

At the same time, institutionally, AGs may be in a better position to engage independent policymaking because AG offices are more likely to resist capture than federal agencies.[344] Because there are many AG offices, and coalitions of AGs in multistate actions are formed on an ad hoc basis, it is difficult for regulated entities to capture participants in multistate actions. That being said, capture could become a greater issue as AGs raise their profile as national policymakers.[345] Because leading AGs generally hail from a handful of states, regulated entities could focus their lobbying efforts on leading AGs and potentially capture a significant number of multistate enforcement efforts.

Multistate settlements are also subject to the criticism that they are too vague to provide fair notice. Because multistate settlements may incorporate the FTC's structural reform terms, such as the requirement to establish comprehensive information security programs, the same complaint could be lodged about vagueness in multistate settlements. However, multistate settlements weather this criticism better than their FTC counterparts. First, multistate settlements generally require the adoption of more specific safeguards than FTC settlements. Second, multistate actions are premised not only on their UDAP authority but also on more specific data protection state statutes that provide greater notice to regulated parties about what is required. While the FTC heavily relies on its broad Section 5 powers, states have more specific data protection statutes with clearer standards. For example, state data notification laws define when corporations need to notify users of a data breach. State law can shape terms of settlement that are clearer for companies to follow than generalized prohibitions on deceptive or unfair practices.

While multistate settlements might be more specific than their federal counterparts, multistate settlements inject greater uncertainty into national policy by creating a patchwork of regulation, instead of a unified standard.[346] Because multistate actions are made up of ad hoc groups of states, settlements can require different and potentially conflicting provisions between and among settlements, making it difficult for the industry to harmonize the settlements. It is unclear how multistate settlements should be interpreted together because the identity and number of states participating in settlements changes in each case. Because there is no continuity in the states that join a settlement, it is difficult to determine whether future settlements amend the standards set forth in previous settlements or reflect the states' most recent thinking about what constitutes best practices. In contrast, the FTC's body of settlements have greater precedential capacity because of the consistency of the settlement terms and the continuity of the FTC as an institution.[347]

344. *See* Mark Totten, *The Enforcers and The Great Recession*, 36 CARDOZO L. REV. 1611, 1611 (2015).

345. *See* Eric Lipton, *Lobbyists, Bearing Gifts, Pursue Attorneys General*, N.Y. TIMES, Oct. 29, 2014 at A1.

346. *See* Turk, *supra* note 37, at 319 (identifying a multi-enforcer problem with regulation by settlement).

347. *See* Solove & Hartzog, *supra* note 10, at 624.

Multistate settlements are even more vulnerable than FTC settlements to the criticism that they create inaccessible standards. Multistate groups generally do not maintain an internet archive of settlements easily accessible to regulated entities and legal professionals.[348] Multistate settlements also do not always include complaints, and companies have to piece together information from press releases, complaints, and settlements scattered across multiple AGs' websites. AG offices also often fail to provide guidance on enforcement such as closing letters for cases they do not pursue, which would give corporations a better understanding of what types of cases are not actionable. It is likely that only large companies with sophisticated counsel have the resources to access multistate settlements to discover a pattern of regulation.[349]

Multistate settlements regulate data practices; however, attributes of multistate enforcement raise unique concerns about regulation by settlement. Because AGs are likely to continue to play an active role in data enforcement, proposed reforms should be considered that specifically address regulation by multistate settlement.

C. Proposed Reforms for Regulation by Multistate Settlement

AGs have provided an important service to consumers by instigating greater data protections and multistate enforcement actions will likely continue to play an important role in national data regulation. Reforms to regulation by multistate settlement can increase transparency and participation in the settlement process and improve accessibility to multistate settlements. Such reforms include notice and comment procedures and providing more information about multistate enforcement actions. AGs should encourage regulation through legislation and state rulemaking as opposed to solely relying on enforcement settlements. Improved judicial oversight also can address concerns about regulation by multistate settlement.

First, greater procedural protections increase transparency and participation in the multistate settlement process. Multistate settlements should have notice and comment periods like FTC settlements before finalization. These procedures would allow stakeholders to participate in commenting on the structural reforms in the settlement. AGs would be better informed about industry standards, especially in areas like data protection that are rapidly changing, if they engaged more stakeholders in the settlement process.

348. *See* Dishman, *supra* note 45, at 342.

349. Large law firms are opening AG practice groups to be a resource for corporations that are targeted by AG and multistate actions. These groups are often led by former AGs and assistant AGs. *See* David Thomas, *O'Melveny Joins Rush to Form State AG Practices as It Fights for J&J in Opioid Cases*, LAW.COM (Oct. 28, 2019), https://www.law.com/americanlawyer/2019/10/28/omelveny-joins-rush-to-form-state-ag-practices-as-it-fights-for-jj-in-opioid-cases.

Because multistate actions are made up of ad hoc groups of AGs, it may be a challenge to create an accessible, permanent platform for notice and comment, like the FTC's website. However, the NAAG has ongoing working groups that have websites where a multistate group could post a proposed settlement for public comment.[350] In the alternative, AGs could partner with the FTC to host multistate settlements on the FTC's website, creating a more unified source of consumer protection settlements. AGs could also post proposed settlements on their own websites and seek public comment. This method may be less accessible, but sufficiently high-profile proposed settlements may drive traffic to the websites for public comment and participation. AGs are particularly well-suited to be responsive to public comment because they are democratically elected. AGs could better balance consumer and business interests if settlements were more accessible to the public and stakeholders before being finalized.

AGs should also increase transparency and participation by engaging in other signaling about their enforcement. For example, AGs should release complaints with settlements so the public can better understand the conduct that led to the enforcement action. Complaints are issued in certain multistate actions in press releases, but it is not a general practice. Further, AGs should provide closing letters for investigations in which they did not pursue enforcement action or seek a settlement, thus providing guidance about corporate practices that did not trigger enforcement action and which corporate compliance programs and remediations were adequate. For example, the FTC issues closing letters in cases where the agency believes the corporation has undergone sufficient remediation.[351] Leading AGs could also issue public closing letters in investigations to give industry greater guidance on remediation efforts that prevent AGs from seeking a multistate settlement.

Second, and relatedly, making multistate settlements more accessible would increase their transparency and stakeholder participation. Greater accessibility would also provide better guidance to companies, particularly smaller businesses that cannot devote the resources to hire lawyers to scour state AG websites for information about multistate settlements. Traditionally, multistate settlements have been difficult to access. The fact of the settlement may appear in the news or in a press release, but these reports often focus on the amount of settlement and not the structural reforms. Some AG offices include a copy of the settlement with the press release, but others do not, which requires visiting multiple AG offices' websites to locate a copy of the settlement. Since multistate settlements are not always required to be filed with courts, court

350. For example, there is an Internet Safety/Cyber Privacy and Security Committee of the NAAG. *See* NAT'L ASS'N ATT'YS GEN., *Internet Safety/Cyber Privacy and Security Committee*, https://www.naag.org/committee/internet-safety-cyber-privacy-and-security-committee (last visited Mar. 7, 2021).

351. *See* Letter from David Vladeck to Albert Gidari, *supra* note 81.

dockets may not contain the settlements. AG offices do not always archive past settlement agreements on their websites, particularly when a different AG has been elected to the office.

Importantly, the NAAG has made efforts to create a database of multistate settlements.[352] Individual AG offices should also make settlement information available to the public. The more accessible the information, the more likely that the settlements will generate public and stakeholder conversations. It would increase predictability for the future if companies had better access to previous complaints, settlements, and other guidance in a centralized forum.

Third, AGs should encourage regulation of corporate conduct through legislation and rulemaking in their own states as opposed to regulating solely through enforcement. AGs are already taking a leadership role in lobbying their state legislatures to pass data protection legislation including data breach notification laws and comprehensive data privacy and security statutes.[353] AGs also have rulemaking powers under certain state statutes such as California's new CCPA.[354] The Attorney General has been active in rulemaking under the CCPA.[355] The California Office of Administrative Law approved new consumer privacy regulations previously proposed by the California AG under the CCPA. These detailed regulations include requirements for privacy policies for consumer information and training for employees handling consumer information.[356] They also require that companies adopt privacy policies that are easily readable and accessible online.[357] Most recently, the California AG announced additional newly-approved regulations that prohibit companies from burdening consumers from opting out of the sale of their personal information by using confusing language or requiring time-consuming or cumbersome steps to opt-out.[358] California voters recently passed Proposition

352. The NAAG has partnered with Professor Paul Nolette to make AG settlements more accessible to scholars and the public. *See* STATE LITIGATION AND AG ACTIVITY DATABASE, https://attorneysgeneral.org.

353. For a discussion of recent state data privacy laws and proposed legislation, see Kessler, *supra* note 12, at 126–27.

354. *See* California Consumer Privacy Act, CAL. CIV. CODE § 1798.185 (West 2020). In contrast, the new Virginia Consumer Data Protection Act (VDCPA) does not provide the Attorney General with express rulemaking authority. *See* Rafael Reyneri & Libbie Canter, *Virginia Enacts Comprehensive Privacy Law* (Mar. 4, 2021), https://www.insideprivacy.com/data-privacy/virginia-enacts-comprehensive-privacy-law.

355. *See* Press Release, *Attorney General Becerra Announces Approval of Additional Regulations to Empower Data Privacy Under the California Consumer Privacy Act* (Mar. 15, 2021), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-additional-regulations-empower-data [hereinafter California AG Press Release].

356. *See* CAL. CODE REGS. tit. 11, § 999.308; § 999.317 (2020).

357. *See* § 999.308.

358. *See* California AG Press Release, *supra* note 355.

24, the California Privacy Rights Act, that expands the CCPA and will ultimately transfer rulemaking from the California AG to an new state privacy agency.[359]

When state statutes and regulations require specific privacy policies, states can effectively expand FTC enforcement jurisdiction. The FTC can bring enforcement actions based on "deceptive acts" under its Section 5 powers when companies make misrepresentations in their privacy policies.[360] Settlements that require a particular company to establish privacy policy do not bind every company, but a state regulation that applies universally would effectively expand the FTC's jurisdiction in a way that individual settlements cannot.

Engaging in rulemaking provides clearer standards for companies to follow than piecing together a mishmash of multistate settlements. If Congress is not going to pass comprehensive federal data legislation or give the FTC traditional APA rulemaking abilities under Section 5, it may be more beneficial for regulated entities to have state laws and rulemaking because it may be a clearer form of regulation, even if there are multiple standards to review and follow. Having clearer state standards for industry may be better than a vague national standard set forth in an FTC settlement. AGs should consider collaboration with other states as they exercise their rulemaking ability to harmonize or at least not create outright conflicting regulations.

Fourth, state courts could play a greater role in overseeing multistate settlements. AG settlements should be required to have judicial approval before they are finalized. This would make the settlement process more transparent. If AGs know that they face enhanced judicial scrutiny at the time of settlement, their behavior in negotiating the settlement would change. Allowing a judicial check would help address the problem of consolidating too much power in the AG because a judge would also have to be satisfied that the settlement was a fair application of state law. Because AGs have considerable leverage, particularly in the multistate context, judicial review could act as a check on AG national policymaking. Enhanced judicial involvement may also address the problem of ongoing monitoring of multistate settlements. Settlements could be entered like court injunctions where corporations violating the terms of the settlement would cause the case to be immediately reopened, as opposed to the AG bringing a new action to enforce the terms of the settlement.

Reforms can increase transparency, participation, and accountability in regulation by multistate settlement. Such reforms can mitigate concerns about this unique form of national regulation and allow AGs to continue to play an important role in data enforcement and regulation.

359. The change in the law will be operative in 2023. *See* Stacy Gray et. al, *California's Prop. 24, The "California Privacy Rights Act," Passed. What's Next?* (Dec. 17, 2020), https://fpf.org/blog/californias-prop-24-the-california-privacy-rights-act-passed-whats-next.

360. *See* Solove & Hartzog, *supra* note 10, at 598–99.

CONCLUSION

AGs have provided an important service to consumers by stepping into a regulatory void in data protection through actively pursuing multistate enforcement actions. Structural reforms in multistate settlements create de facto national regulations. However, unique concerns arise in the context of regulation by multistate settlement. These concerns can be addressed by increasing participation, transparency, and judicial oversight in the multistate settlement process.