Note

"Key" Tam: Giving Teeth to Federal Data Security Enforcement

Brandon Stottler∗

Data breaches wreak havoc on data-handling entities, weigh heavily on the minds and hearts of breach victims, and elude the efforts of regulators and scholars alike. Since 2005, declared the "Year of the Data Breach," every year has seen an increase in the number and impact of breaches. Data breaches cost United States companies billions of dollars, undermine consumer confidence, exacerbate geopolitical tensions, increase anxiety, and even result in bodily harm and death. Nevertheless, a suitable federal framework has yet to be enacted to address the perennial problem. Though the data breach epidemic may seem like a recent phenomenon—a biproduct of the current data-dependent internet society—data privacy and security concerns have existed as early as the first United States Census. Through a process of innovation-and-response, the regulatory framework has developed into a haphazard patchwork of industry-specific standards that baffle both entities and consumers. Meanwhile, attempts to recover damages through civil actions are rarely successful in the face of procedural barriers, and the majority of federal data breach enforcement comes under a century-old law.

This Note proposes that qui tam—an enforcement mechanism that allows private individuals called "relators" to sue on

---

∗ J.D. Candidate 2025, University of Minnesota Law School; Note & Comment Editor, *Minnesota Law Review* Volume 109. Thank you to all who helped me produce this Note, including, but not limited to: Professor Daniel Schwarcz for his thoughtful and diligent advising; Ryan Liston for his guidance throughout the writing process; Kaz Lane, Samuel Makikalli, Mark Hager, and Callan Showers for their hard work throughout the editing process; and Noah Alvarado, Kylie Lewis, Thomas Murray, Nico Patch, Josh Ryan, and Eliza Schueneman for their careful cite-checking.

behalf of the Government to vindicate public rights—would serve to address many of the issues that plague data breach enforcement. This Note argues that qui tam mechanisms should be included in federal data security legislation to properly address the underenforcement issues and barriers to successful litigation that allow the age of the data breach to rage on. It further analyzes the current use of qui tam mechanisms in the False Claims Act as recently applied to government data contractors. Finally, it proposes two possible applications of qui tam: first, applying qui tam to a data security statute under a theory of the relator as an agent of the Government; and second, applying qui tam under the theory of the relator as a partial assignee of the Government's claim. These proposals allow for better oversight and enforcement of data security standards to put the age of the data breach in society's rearview mirror.

INTRODUCTION

By now, the story is familiar. While applying for a job, for college, or for a credit card to get ten percent off the latest impulse purchase, "Ol' Trusty, Inc." asks CJ[1] for her Social Security Number (SSN), and though she hesitates, the screen gives assurance: "*Your privacy matters to us*." So, CJ types in her nine-digit passcode-to-the-world and moves on with her life.

A few years later, CJ pauses on a news story while sleepily scrolling social media and sipping coffee. The title reads: "Over 7 Million SSNs Potentially Exposed in Ol' Trusty Breach."[2] "Of course," CJ mumbles as she scrolls on—this is just one of many similar breach headlines she has already seen this year.[3] A month later, CJ receives an email from Ol' Trusty, warning her that her information could have been exposed as a result of the breach.[4] Another month passes, and CJ receives another email: her personal information *was* exposed. The anxiety sets in for CJ: *Who has my information? What are they going to do? What have they already done?* The email reassures: "*Your privacy matters to us*." The words, at one point hollow and harmless, now feel mocking and sardonic. Ol' Trusty offers CJ a year of credit-monitoring software,[5] but the initial harm is done. CJ is left with persistent anxiety of what might happen now that she is among the exposed.

---

1. For the purposes of this Note, CJ is a hypothetical "Citizen Jo," an amalgamation of victims of similar stories affected by data breaches; "Ol' Trusty, Inc." is a fictional entity. *See infra* notes 2–11 and accompanying text.

2. *See, e.g.*, Ashish Khaitan, *Over 7 Million SSNs Potentially Exposed in University of Minnesota Data Breach*, CYBER EXPRESS (July 21, 2023), https://thecyberexpress.com/university-of-minnesota-data-breach [https://perma.cc/PS8U-35HU] (providing an example of a major data breach that exposed potentially millions of Americans' SSNs).

3. *See* Sam Sabin, *2023 Toll of Data Breaches and Leaks Already Tops 2022*, AXIOS (Oct. 13, 2023), https://www.axios.com/2023/10/13/2023-data-compromises-surpass-2022 [https://perma.cc/9KZM-LEVN] (reporting that the total number of data breaches and leaks in 2023, as of October, totaled 2,116).

4. *See, e.g.*, Alex Lassiter, *UMN Sued After Data Breach Incident*, MINN. DAILY (Sept. 17, 2023), https://mndaily.com/278440/campus-administration/campus/umn-sued-after-data-breach-incident [https://perma.cc/RTX4-KJXM] (providing an example of a university notifying the victims of a major data breach by email).

5. *See, e.g.*, Sasha Romanosky et al., *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 90 (2014) (noting that "credit monitoring is widely touted as a best practice following a data breach" and citing three examples).

For many, this story is all too familiar. For example, David Anderson, a business school professor, knows of four times that his personal data has been stolen—though, in all truth, it has probably been more.[6] Anderson has been "lucky," as his information has not yet been used against him.[7] Many are not so lucky.[8] Some breach victims have their credit ruined as a result, leaving them unable, for example, to secure much-needed mortgage refinancing.[9] Others like Janis Barbour, a retired market researcher, spend months dealing with the administrative burden of fraud only to be punished with another breach notification.[10] Many others are left in a ceaseless pattern of fraud attempt notifications, unrequested two-factor authentication requests, and frantic password resets.[11] Data breaches[12] have become commonplace and leave victims with an anxious feeling of uncertainty. The growing phenomenon has sparked heavy

6. Tiffany Hsu, *Data Breach Victims Talk of Initial Terror, Then Vigilance*, N.Y. TIMES (Sept. 9, 2017), https://www.nytimes.com/2017/09/09/business/equifax-data-breach-identity-theft-victims.html [https://perma.cc/NC4Z-V68F] (noting multiple massive data breach attacks, including one which exposed the personal information of 143 million Americans).

7. *Id.*

8. Data suggests a strong correlation between breaches and identity theft—victims of identity theft are over twice as likely as nonvictims to learn that their personal information was exposed in a data breach in the past year. Erika Harrell, *Just the Stats: Data Breach Notifications and Identity Theft, 2021*, BUREAU JUST. STAT. (Jan. 2024), https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021 [https://perma.cc/UFY3-A2FP].

9. *See* Hsu, *supra* note 6 ("One man said the thieves had so ruined his credit, he was unable to secure a needed mortgage refinance.").

10. *Id.* Barbour spent nine months attempting to resolve an instance of tax fraud with the Internal Revenue Service (IRS), only to later receive a notification that her personal information was again exposed in the Equifax breach of 2017. *Id.*

11. *See id.* (discussing the personal challenges and inconveniences that data breach victims face, including "discoveries months later that there's another account you have to correct").

12. Though definitions of "data breach" vary subtly from jurisdiction to jurisdiction, the sentiment remains largely similar. For purposes of this Note, a "data breach" is the "loss of control, compromise, unauthorized disclosure, [or] unauthorized acquisition . . . where a person other than an authorized user accesses or potentially accesses personally identifiable information (PII); or an authorized user accesses or potentially accesses PII for an [other-than-authorized] purpose." U.S. DEP'T OF JUST., ORDER NO. 0601, PRIVACY AND CIVIL LIBERTIES 4 (2020); *see also* CAL. CIV. CODE § 1798.29(f) (West 2023) (providing a similar definition of data breach); 38 C.F.R. § 75.113 (2023) (providing a similar definition of data breach, but also highlighting the theft of information).

concern over data privacy and security and has even resulted in some new laws that aim to empower consumers with information regarding breaches.[13] Despite all the attention, however, breaches are not going away.[14]

Even though modern data breach concerns seem novel in the context of the internet age, privacy concerns have been central to American values since colonial times.[15] Even the concepts of data privacy and security are not entirely new, with "public outcr[ies]" arising over the sharing of personally identifiable information as early as the 1890 U.S. Census.[16] As the country's population expanded and new technologies developed, concerns about data privacy and security also grew—as did legislation aimed to address the concerns.[17] The rise of the internet in the 1990s exacerbated these concerns, complicating discussions on how to balance the benefits that flow from the use of personal data with the potential risks to both individuals and society.[18]

Scholars generally agree that the current framework of data privacy and data security law is a haphazard and marginally-effective patchwork of statutes and common law.[19] Tangible solutions to rein in the now ubiquitous and infamous data breach

13. *See, e.g.*, DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 35–43 (2022) (discussing notification and disclosure laws).

14. *See, e.g.*, *id.* at 29 (providing a chronology of data breaches, noting that "the general trend is more breaches and compromised records with no improvement in sight").

15. *See generally* Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY 1-1 (Kristen J. Matthews ed., 2006 & Supp. 2016) (presenting a history of information privacy law in the United States, from colonial America to the twenty-first century).

16. *Id.* at 1-6 (noting that questions about diseases, disabilities, and finances in the 1890 census spurred a public outcry that ultimately led to stricter confidentiality laws); *see also* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 669 (2013) (noting the histories of and distinctions between privacy law and security law).

17. *See infra* Part I.B (providing a brief history of the development of privacy and security laws in the United States).

18. *See* Solove, *supra* note 15, at 1-36 (discussing the rise of computer technologies through the 1990s, such as "cookies" and "web bugs," to identify users and create salable marketing data).

19. *See generally, e.g.*, SOLOVE & HARTZOG, *supra* note 13 (discussing critiques of data privacy and security law in the United States).

are particularly elusive.[20] Despite a considerable body of plausible scholarly proposals,[21] data breaches continue to cost United States companies billions of dollars, undermine consumer confidence, exacerbate geopolitical tensions, raise societal anxiety, and may even result in bodily harm and death.[22]

While what's required of data handling entities is clear across myriad sources of law,[23] the timing and effectiveness of the current security framework is inadequate and demands reform. Regulations and legislation provide an underenforced patchwork of varying standards across states and industries, leaving data-controlling entities uncertain of which frameworks apply to them and consumers baffled over methods for recovering from breach incidents.[24] Meanwhile, lawsuits in tort and breach of contract *occasionally* succeed, though Article III

20. *See id.* at 17 ("Policymakers have sprung into action, enacting a myriad of new data security and breach notification laws during the past 15 years. But the problem keeps growing.").

21. *See, e.g.,* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 767–73 (2018) (describing the legal foundations for courts to acknowledge the emotional distress caused by a data breach as a cognizable harm); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 624–26 (2018) (proposing the framework for a "tort of breach of confidence" when data-controlling entities violate their fiduciary-like duty of confidentiality to consumers). *But see* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 520–28 (2019) (critiquing the fiduciary-like duty characterization of data-controlling entities as insufficient to address the problems of data breaches).

22. *See* Daniel Schwarcz et al., *How Privilege Undermines Cybersecurity*, 36 HARV. J.L. & TECH. 421, 424 (2023) (noting the variety of harms resulting from recent breaches); *see also* Sasha Romanosky, *Examining the Costs and Causes of Cyber Incidents*, 2 J. CYBERSECURITY 121, 129–33 (2016) (describing empirically the costs of data breaches on data-controlling entities); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 252–55 (2007) (describing the emotional, financial, and physical harms that modern data theft inflicts upon consumers).

23. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1141–70, 1208 (2019) (providing a comprehensive analysis of the sources of duty in data security laws, which harmoniously conclude that the duty is that of a reasonableness standard). McGeveran's article outlines fourteen frameworks, or sets of requirements, which establish the duties of data security. *Id.* at 1142–43.

24. *See, e.g.*, *id.* at 1143–58 (discussing the different sources of data security laws, including federal sectoral regulation, consumer protection regulation, state laws, and private frameworks).

standing, class certification issues, and the difficulties in determining damages all preclude an adequate disposal of data breach concerns.[25] While the need for federal data security legislation is evident, disagreement over the efficacy of currently-posited enforcement mechanisms has doomed meaningful proposals that aim to address the unique challenges posed by breaches.[26]

Recent scholarly interest in qui tam, an enforcement mechanism that enables private individuals to sue on behalf of the Government to vindicate public rights, suggests that this once-obscure mechanism is potentially a viable tool in federal data security legislation to address the deterrence and prevention of breaches.[27] These actions allow for broader public enforcement through private monitoring without the Article III standing or class certification issues of private rights of action.[28] In doing so, qui tam grants the relating party a portion of the Government's damages should the Government pursue and succeed in the lawsuit.[29]

The Supreme Court has recently upheld the validity of qui tam provisions as enforcement mechanisms, paving the way for future use despite the current scarcity of such provisions in

---

25. *See id.* at 1144–45 (noting several of the procedural barriers that litigants face in data breach lawsuits and the subsequent court rulings that fail to reach a case's merits); *see also* Transunion LLC v. Ramirez, 141 S. Ct. 2190, 2203–14 (2021) (analyzing the requirements of Article III standing and applying them to plaintiffs' suit of a credit reporting agency under the Fair Credit Reporting Act).

26. *See, e.g.*, SOLOVE & HARTZOG, *supra* note 13, at 67–68 (positing that, by focusing too much on the breach itself, data security law fails to address both the preventable causes and harmful effects of the breach); *see also* JONATHAN M. GAFFNEY ET AL., CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152, at 1, 2–3 (2022) (highlighting the disagreement over the American Data Privacy and Protection Act's (ADPPA) enforcement mechanism that ultimately stalled its passing).

27. Myriam Gilles & Gary Friedman, *The New Qui Tam: A Model for the Enforcement of Group Rights in a Hostile Era*, 98 TEX. L. REV. 489, 491 (2020) (examining the possibility of qui tam actions as an expansion of state police power on data breaches).

28. *See* Peter Ormerod, *Privacy Qui Tam*, 98 NOTRE DAME L. REV. 267, 312–15 (2022) (discussing the procedural advantages of qui tam in avoiding standing and class certification).

29. *See infra* Part II.

federal statutes.[30] Further, in October 2021, the United States Department of Justice—aiming to employ the qui tam provision of the False Claims Act to bolster federal enforcement of data security measures—announced a Civil Cyber-Fraud Initiative (CCFI).[31] In addition, recent proposals have argued for the use of qui tam in new privacy laws, advocating for a framework of privacy as a public right.[32]

This Note analyzes the viability of qui tam provisions as a potential solution to the enforcement woes that have plagued data security laws in the United States.[33] Such laws that specifically address data breaches have three primary goals: to deter and prevent breaches themselves, to identify and compensate victims of breaches, and to reduce the harm from breaches.[34] This Note focuses primarily on the deterrence and prevention of

30. *See* Vermont Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 775 (2000) (holding that relators in qui tam suits have Article III standing); United States *ex rel.* Polansky v. Exec. Health Res., Inc., 143 S. Ct. 1720, 1727–30 (2023) (providing a history of qui tam in the United States and resolving a circuit split in favor of allowing the Government to dismiss False Claims Act qui tam actions over a relator's objection). *But see* United States *ex rel.* Zafirov v. Florida Med. Assocs., LLC, No. 19-cv-01236, 2024 WL 4349242, at *20 (M.D. Fla. Sept. 30, 2024) (relying heavily on Justice Thomas's dissent in *Polansky* to hold that qui tam is unconstitutional).

31. Press Release, U.S. Dep't of Just., Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative [https://perma.cc/8MG6-TKEB] (announcing a "Civil Cyber-Fraud initiative" intended to promote cyber security enforcement through private whistleblowers).

32. *See* Ormerod, *supra* note 28, at 316 (arguing for a qui tam privacy law proposal that interprets privacy as a social phenomenon rather than the more traditional individual "right to be let alone"); *see also infra* notes 283–84 (discussing Ormerod's framework).

33. This Note was partially inspired in consideration of Ormerod's proposal for a "Privacy Qui Tam." *See infra* notes 283–84. However, Ormerod's proposal requires a reframing of privacy as a public right, enforceable by the Government, whereas this Note emphasizes the distinction between privacy and security and proposes a qui tam *security* enforcement mechanism to address breaches as a subdivision of privacy and security law.

34. *See infra* Part I (outlining the approaches to breach laws and the benefits and shortcomings); *see also* Robert L. Rabin, *Perspectives on Privacy, Data Security, and Tort Law*, 66 DEPAUL L. REV. 313, 318 (2016) (noting the lack of consensus on appropriate mechanisms to punish breaches, prevent breaches, compensate victims, and reduce harm); McGeveran, *supra* note 23, at 1138 (noting that the law still struggles with measuring harm and damages in data breach cases).

breaches, keeping in mind that reduction of harm is necessarily addressed in reducing the prevalence of breaches.[35] Specifically, this Note argues that most laws that attempt to address data breaches are inadequate because they are enforceable only *after* a breach occurs.[36] This Note also argues that a principal benefit of qui tam security enforcement is that it can address security deficiencies earlier than traditional enforcement strategies.[37] It further argues that qui tam would be most successful as an integrative,[38] "win-win" enforcement mechanism to help curtail the breach epidemic when tied to a federal certification scheme as a means to empower those with knowledge of security deficiencies to take legal action, though it may also be successful when tied to federal interests in securing citizens' personal data.[39]

This Note makes its argument in three Parts. Part I provides an overview of data privacy and security law in the United States and surveys the current legal landscape in the context of

---

35. The reduction of breaches would presumably make it easier to identify and compensate victims of breaches as well, as fewer breaches mean fewer victims. Further, rewards from successful qui tam litigation may be used to fund victims' compensation funds, thus addressing the second purpose as well, though this analysis is largely outside the scope of this Note. For further discussion, see Marian K. Riedy & Bartlomiej Hanus, *Yes, Your Personal Data Is at Risk: Get over It!*, 19 SMU SCI. & TECH. L. REV. 3, 37–40 (2016) (discussing the viability of an administered compensation fund for victims).

36. *See* SOLOVE & HARTZOG, *supra* note 13, at 53 (noting that the majority of breach law enforcement actions are triggered by the occurrence of a breach, inflicting more difficulty on an already struggling entity).

37. *See infra* Parts I.C.1, II.B (discussing how qui tam enforcement allows earlier detection of security deficiencies by employing private actors with closer knowledge of firm's security practices to file suits on behalf of the Government).

38. This Note borrows the definition of "integrative" from negotiation theory to indicate scenarios that offer win-win outcomes. *See, e.g.*, *Types of Negotiation*, HARV. L. SCH.: PROGRAM ON NEGOT., https://www.pon.harvard.edu/tag/types-of-negotiation [https://perma.cc/A9Q5-4GT9] (describing an integrative negotiation as "win-win" because "there is more than one issue to be negotiated, and negotiators have the potential to make tradeoffs across issues"). This Note argues that, because breaches negatively impact both data subjects and data-controlling entities, security enforcement before the breach offers a win-win situation; while companies may face liability before the breach, the potential penalty likely pales in comparison to the cost of an actual breach. *See infra* Part I.C (discussing the cost of data breaches on data-controlling entities); *see also infra* note 82 and accompanying text (discussing the same).

39. *See infra* Part III.A (setting forth two proposals for qui tam in a federal data security statute). This Note takes the position that while both proposals would be effective, the certification scheme would be preferable because it allows for enforcement before any breach need occur. *See infra* Part III.A.

data breaches. Specifically, this Part: (1) distinguishes between privacy and security law and explains why that distinction matters; (2) addresses the current enforcement challenges of traditional privacy and security laws; and (3) outlines recent shifts and popular proposals in data protection laws. Part II then turns to qui tam, beginning with an overview of qui tam enforcement mechanisms in American law, followed by a discussion of the qui tam action of the False Claims Act and its recent application to data security. The second half of Part II focuses on qui tam's recent resurgence as a respected enforcement tool. Part III puts forth a proposal of security qui tam enforcement provisions as an effective enforcement strategy in the context of data protection laws by outlining two viable applications. It concludes with an analysis of the promises of qui tam in data security enforcement.

I. DATA PRIVACY AND SECURITY LAW IN THE UNITED STATES

An understanding of the state of privacy and security law in the United States—and the difference between the two—is crucial to understanding (1) why data security is the correct focus for breach enforcement, and (2) how qui tam mechanisms can bolster the data security regime. This Part analyzes the regime in four Sections. The first Section sets forth an important distinction between "privacy" and "security." The second Section provides an overview of security law in the United States to provide a framework for the issues this Note seeks to address. Finally, the last two Sections offer a critique of both the current regime and recently proposed solutions.

A. SECURITY VERSUS PRIVACY

As a preliminary matter, considering how to properly deal with issues arising from the widespread use of data requires awareness of the distinction between privacy and security. This is because, while overlapping, each respective legal domain differs in scope and poses distinct normative barriers to passing legislation.[40] To properly enact data breach enforcement through

40. *See* SOLOVE & HARTZOG, *supra* note 13, at 133–38 (discussing the "schism" between privacy and security). *See generally* Bambauer, *supra* note 16 (discussing the differences between privacy and security in legal scholarship).

qui tam-inclusive legislation, it is first necessary to determine which domain best effectuates the goals of data breach laws.[41]

Essentially, privacy involves normative choices about who has, and who should have, legitimate access to use and alter personal information.[42] Security, in contrast, implements those decisions and mediates between competing choices and interests in information.[43] Questions of privacy law include, but are not limited to: who actually owns personal information such as SSNs; how personal information can be traded; who has legitimate interests in personal information; how to balance the competing interests of the economic value of data in increasing efficiency and the values of autonomy; and whether safety or privacy is more important.[44] On the other hand, security law determines who can actually access, use, and alter data, as well as what kind of safeguards they must employ while doing so.[45] Security law is "agnostic" to the normative questions of who *should* have access, instead focusing on who *does* have access, and what responsibilities, or duties, they have when handling that data.[46] For example, the question of whether an entity should ask for and retain customers' email addresses is a privacy question; if the entity accidentally makes those addresses publicly available on its website, it is a security problem.[47]

The distinction between privacy and security is important because it means that privacy is a zero-sum game, while security may have integrative solutions.[48] In other words, questions of

41. *See supra* note 34 and accompanying text (listing the goals of breach laws as "to deter and prevent breaches themselves, to identify and compensate victims of breaches, and to reduce the harm from breaches").

42. Bambauer, *supra* note 16, at 683 ("Privacy discourse involves difficult normative decisions about competing claims to legitimate access . . . .").

43. *Id.* at 669 ("Security defines which privacy choices can be implemented.").

44. *See generally id.* (discussing the various questions with which privacy law must contend).

45. *Id.* at 669 (defining security as the set of mechanisms that work to enact privacy protections and mediate requests for access and control).

46. *Id.* at 676–78 (discussing data security and its interaction with privacy).

47. *Id.* at 679 (discussing the data incident where Biofilm, a company that makes and sells personal lubricant, inadvertently disclosed its customers' email addresses).

48. *Id.* ("From a utilitarian perspective, privacy issues are a zero-sum game . . . . Security issues, by contrast, result in an outcome that is worse for

privacy have push-and-pull, such as the aggregate economic benefit to data-controlling entities of possessing and using users' personal information at the expense of that information's disclosure.[49] Meanwhile, security issues result in breaches—"an outcome that is worse for both sides."[50] A data breach imposes significant costs on the data-controlling entity even beyond potential litigation and penalties, such as repairing infrastructure, damage control, and reputational harms, to name a few.[51] Breaches also cost the users in the form of anxiety, at minimum, as well as risks of fraud and identity theft.[52] Speaking generally, data breaches leave everyone worse off.[53]

Taken together, the distinction between privacy and security combined with the current challenges of breach enforcement suggests that laws seeking to minimize breaches, and the associated harms, should focus on security rather than privacy.[54] Security-centered breach laws allow legislators to sidestep the normative arguments of privacy law and focus on integrative solutions that are less susceptible to pressure from adversarial constituents.[55] Breaches benefit no one—except, perhaps, identity thieves and fraudsters. Thus, any proposed law hoping to remedy the breach epidemic should be focused on security and tailored to integrative solutions.[56] With security in mind, the

---

both sides."); *cf. The Program on Negotiation*, *supra* note 38 (explaining that the term "integrative" indicates a potential for win-win outcomes).

49. Bambauer, *supra* note 16, at 674–75, 679 (discussing the economic benefit to entities of collecting information for marketing purposes).

50. *Id.* at 679.

51. SOLOVE & HARTZOG, *supra* note 13, at 129–35 (discussing the costs of breaches to entities).

52. *See supra* notes 8–11 and accompanying text (discussing harms to breach victims).

53. *See supra* notes 8–11, 82 and accompanying text; Bambauer, *supra* note 16, at 681 (noting that "security failures" leave everyone except the attacker worse off).

54. *See infra* Part I.C (addressing issues with current breach enforcement laws).

55. *See infra* note 253 and accompanying text (discussing how disagreement over normative issues has in part stalled federal data privacy and security legislation).

56. *See infra* notes 85–86 and accompanying text (discussing how current enforcement mechanisms, when successful, punish data-controlling entities while they are already dealing with the high economic and reputational costs of a data breach, suggesting the current regime is adversarial rather than integrative).

next Section provides a history and overview of security laws in the United States to give context for this Note's proposal.

B. AN OVERVIEW OF DATA SECURITY LAWS IN THE UNITED STATES

While the recent explosion of the data economy spurred by the internet revolution has forcibly shoved data security into the societal consciousness as a central issue of the day, the general principles and approaches toward federal security law have remained the same for nearly a century.[57]

The invention of the telegraph in 1844 catalyzed this ongoing battle between privacy, security, and technology.[58] Despite rigorous debate over the proper legislative response to the privacy concerns that the telegraph wrought, it took Congress nearly forty years to introduce a bill to address the privacy protection of telegrams—and the bill failed to pass.[59] However, a majority of states passed their own laws prohibiting the disclosure of telegraph messages by telegraph company employees.[60] The telephone's invention in 1876 garnered similar results, with states enacting laws where Congress failed to act.[61]

In 1934, Congress finally enacted section 605 of the Federal Communications Act, a privacy-focused law that effectively prohibited all parties except the sender and intended recipient(s) from accessing communications over telegraph and telephone.[62] Around the same time, Congress created the Social Security System, providing for the assignment of a unique Social Security Number (SSN) to every American citizen.[63] Initially meant to be used only for administration of the system, the use of SSNs

57. Solove, *supra* note 15, at 1-19, 1-24 to 1-45 (summarizing the evolution of privacy law in various bills over the last century).

58. *See id.* at 1-7 ("Shortly after the telegraph's invention in 1844, technology to tap into telegraph communications emerged." (footnote omitted)).

59. *Id.* at 1-8 ("A bill to protect the privacy of telegrams was introduced into Congress in 1880. The bill would ultimately be abandoned." (footnote omitted)).

60. *Id.* ("More than half the states enacted laws.").

61. *See id.* at 1-18 (discussing state responses to privacy concerns over telephone communications).

62. *Id.* at 1-19 ("[N]o person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person . . . ." (quoting 7 U.S.C. § 605 (repealed 1947))).

63. *Id.* at 1-18.

would explode into its current status as "the worst password ever created."[64]

From there, a pattern of innovation-and-response led to the current state of data security law. The computer burst onto the scene in 1946 and revolutionized information collection and processing.[65] Over the next seven decades, the amount of collected data ballooned as computer technology developed.[66] In response to each development, new, mostly sectoral data privacy and security laws developed as well.[67] However, these new laws largely enforced the same privacy-centered principle of section 605 of the Federal Communications Act: that information should only be accessed and used by those for whom it is intended.[68]

The "Age of the Data Breach" unofficially began in 2005, when multiple data brokers announced that their records or

64. SOLOVE & HARTZOG, *supra* note 13, at 119; *see also* Solove, *supra* note 15, at 1-26 to 1-27 (noting that efforts to rein in the use of SSNs as personal identifiers have largely failed, with SSNs still often used as passwords and identifiers across government, employment, financial, educational, and medical sectors).

65. *See* Solove*, supra* note 15, at 1-24 ("[T]he computer revolutionized the way records and data were collected, disseminated, and used.").

66. *See id.* at 1-24 to 1-30 (discussing the various ways in which computers increased the amount of data collected about individuals).

67. *See id.* at 1-24 to 1-45 (discussing legislative responses). While the laws largely enforced similar principles, they began to refer to "information" in its discrete form as "data." Most of these laws trace back to a 1973 report by the United States Department of Health, Education, and Welfare which outlined a set of "Fair Information Practice Principles" (FIPPs) that set a standard for security safeguards. *Id.* at 1-25 to 1-26 (citing SECY'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC., & WELFARE, (OS) 73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 29 (1973)). This early legislation included the Family Educational Rights and Privacy Act (FERPA) in 1974 for education records, as well as the Cable Communications Policy Act (CCPA) and Video Privacy Protection Act (VPPA) in the 1980s to protect the disclosure of Americans' viewing habits. *Id*. at 1-27 to 1-34. In the 1990s, Congress passed the Driver's Privacy Protection Act of 1994 (DPPA) for protection of motor vehicle records; the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for health records; the Children's Online Privacy Protection Act of 1998 (COPPA) for personal information of children on the internet; and the Gramm-Leach-Bliley Act of 1999 (GLBA) for third-party financial records. *Id.* at 1-37 to 1-39.

68. *See supra* note 67 (discussing the various laws enacted to address different privacy concerns).

systems were breached.[69] Since then, experts have observed a "general trend [of] more [data] breaches and compromised records with no improvement in sight."[70] In response, every state in the U.S. has passed a basic breach notification law,[71] with a few states passing more stringent laws outlining privacy and security standards.[72] Still, a vast majority of data security enforcement at a national level occurs in one of two ways: (1) through the issuance of consent decrees by the Federal Trade Commission (FTC), authorized by a century-old law that prohibits "unfair or deceptive acts or practices,"[73] or (2) through private

69. *See* SOLOVE & HARTZOG, *supra* note 13, at 18 ("Before 2005, there were certainly many data breaches, but companies weren't required to report them . . . . In 2005, light began to shine on the dark underworld of data security."). ChoicePoint was one of the first companies to announce publicly that a breach occurred. *Id.*; *see also* Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress, (Jan. 26, 2006), https://www.ftc.gov/news-events/news/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million-civil-penalties-5-million-consumer [https://perma.cc/6W5P-NW7Y] (noting that 800 cases of identity theft were linked to the company's breach). Four major companies disclosed data breaches the following month. SOLOVE & HARTZOG, *supra* note 13, at 39.

70. SOLOVE & HARTZOG, *supra* note 13, at 29.

71. Brad N. Greenwood & Paul M. Vaaler, Do US State Breach Notification Laws Decrease Firm Data Breaches? 1 (Mar. 9, 2023) (unpublished working paper) (on file with the *Minnesota Law Review*). Breach notification laws require that an entity who has been subject to a data breach—wherein collected personal information is potentially exposed—notify every potential victim. SOLOVE & HARTZOG, *supra* note 13, at 39–42.

72. Most notably, California has passed the California Consumer Privacy Act (CCPA), which requires disclosure of how data will be used and grants some rights to consumers surrounding their data. *See* CAL. CIV. CODE § 1798.105(a) (Deering 2023) ("A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.").

73. *See* PETER SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 44–52 (3d ed. 2020) (discussing FTC data security enforcement); 15 U.S.C. § 45. This is an example of what is generally known as a "security safeguards law." *See* SOLOVE & HARTZOG, *supra* note 13, at 49. Security safeguards laws typically either (1) lay out a set of standards that data-collecting entities must follow or (2) adopt a "reasonableness" approach, requiring entities to protect data with "reasonable," "appropriate," or "adequate" safeguards. *Id.* HIPAA is an example that sets out its own standards, while the GLBA adopts a reasonableness approach. *See* Solove, *supra* note 15, at 1-37 to 1-39 (discussing how HIPAA and the GLBA each operate to protect privacy). Interestingly enough, the FTC often

litigation, with the majority of these cases brought as one of a variety of common law claims.[74] These approaches all share a critical shortcoming: they are typically triggered by a data breach, meaning enforcement is too late to prevent or deter the breaches and resulting harms.[75] The next Section elaborates on this critical timing problem alongside procedural barriers to effective enforcement in the current security law regime.

C. THE CHALLENGES OF TRADITIONAL SECURITY ENFORCEMENT

There are inherent issues with an enforcement regime that requires waiting to act until the harm which one is trying to prevent has already occurred. Notwithstanding this issue, the current regime is underenforced, under-compensates victims, under-incentivizes data-collecting entities to bolster their security practices, and is expensive for the government, companies, and individuals.[76] This Section analyzes these problems with particular focus on timing and procedure.

1. The Timing Issue

Breach notification laws, security safeguard laws, and private litigation all suffer from "an unhealthy obsession with the breach" as some sort of singularity, only *after* which enforcement

---

relies on a set of standards published by the National Institute of Standards and Technology (NIST) in determining whether an approach has been reasonable. SOLOVE & HARTZOG, *supra* note 13, at 51.

74. These claims are as opposed to statutory claims. *See* Romanosky et al., *supra* note 5, at 100 (finding that, in an analysis of 231 cases, there were eighty-six unique causes of action, with "34 different kinds of tort causes of action, 15 contract, 4 violations of state statutes, and 33 violations of federal statutes"). Private litigation seeks to empower victims to pursue redress for harms from breaches while, at the same time, encouraging data-collecting entities to follow strict security measures. SOLOVE & HARTZOG, *supra* note 13, at 55.

75. *See* SOLOVE & HARTZOG, *supra* note 13, at 53, 60–61 (discussing how a strong societal focus on data breaches has led to data security law enforcement that ends up being too late to actually prevent breaches).

76. *See* McGeveran, *supra* note 23, at 1138 (describing some of the challenges of traditional security enforcement including "systematic[] underinvest[ment] in security," and an "[over]reliance on investigations triggered by security failures"); *see also* Rabin, *supra* note 34, at 323 (finding the three main problems of the "current legal regime" to be "(1) uncompensated victims; (2) inadequate incentives for companies and governments to invest in data security; and (3) uncertainty for corporations with respect to their regulatory burdens and litigation risk").

can be brought.[77] While, in theory, these laws all serve to deal with the aftermath of the breach and incentivize data-collecting entities to retain sufficient security standards,[78] the post-breach nature lessens the efficacy of these laws.[79]

For one, notification laws give inadequate protection to the customer because the frequency of breach occurrences often lead to "breach notification fatigue," making it challenging for people to take action.[80] Even when people decide to take action, there is not much they can do—they can change their passwords and keep an eye on their accounts, but changing their fingerprints or SSNs is infeasible.[81] What is left is anxiety and, frequently, a sense of impending identity theft. Furthermore, these laws unnecessarily increase the costs of data-controlling entities by requiring them to investigate and analyze what parties were affected, carefully draft the notifications, and execute massive mailing campaigns.[82] These efforts all take attention and effort away from where it should really be focused: bolstering security and ensuring that breaches do not reoccur.

Safeguard laws—codified laws that set "administrative, physical, and technical data security standards"—are perhaps a step closer to effective data security law, but waiting for the

77. SOLOVE & HARTZOG, *supra* note 13, at 60; *see id.* ("For example, breach notification laws revolve around the breach. Attorneys file hundreds of lawsuits in the wake of a data breach. The FTC and Department of Health and Human Services (HHS) typically use the data breach as the launching point of their enforcement actions.").

78. That is, expenses of litigation or enforcement actions may—in theory—encourage entities to proactively bolster their data security practices.

79. *See supra* note 75 and accompanying text.

80. SOLOVE & HARTZOG, *supra* note 13, at 45 ("Receiving countless notices becomes tiresome, making some people throw up their hands and think that all is hopeless." (citing Bethan Moorcraft, *Are US Consumers Suffering From Data Breach Notification Fatigue?*, INS. BUS. (June 19, 2019), https://www.insurancebusinessmag.com/us/news/cyber/are-us-consumers-suffering-from-data-breach-notification-fatigue-170386.aspx [https://perma.cc/SH5F-XY4M])).

81. *Id.* ("Even when people do receive a notice, there often isn't much they can do about the breach. People can change their passwords and keep an eye on their credit card transactions, but they can't change their fingerprints, and Social Security Numbers are very difficult to change.").

82. *See id.* (discussing the costs associated with a data breach that data-controlling entities bear); *supra* note 71 (describing the notification requirements of security safeguard laws).

breach clearly misses the mark.[83] Despite the issues surrounding enforcement of data security, the actual *duty* of data security in safeguard laws is clear[84]—but waiting for a breach to assess whether data-collecting entities are meeting that duty means that enforcement typically occurs after breach victims' data is exposed.[85] Further, companies that experience breaches are already experiencing the costs and pains of internally responding to the breach—thus, fines that are often only a fraction of the total costs of a breach may be an "exercise in redundancy."[86]

Private litigation as an enforcement mechanism encounters substantially the same issue: enforcement only occurs after cognizable harm, which courts rarely recognize in the breach context,[87] leaving data-controlling entities with limited incentives to bolster their security practices outside of necessary compliance.[88] In other words, litigation as a deterrence mechanism for breaches is inadequate because it "enables [data-holding entities] to evade liability regardless of the level of precautions that they take."[89] Then, when litigation *does* occur in response to a breach, it imposes additional costs—and potentially misallocates valuable resources—at a time where a data-controlling entity's focus and resources should be on internal breach response and bolstering security.[90]

---

83. SOLOVE & HARTZOG, *supra* note 13, at 47; *see also supra* note 73 and accompanying text (defining security safeguards laws and providing examples).

84. *See* McGeveran, *supra* note 23, at 1208 (explaining that the duty of data security is one of reasonableness, requiring that "data custodians assess their security risks and implement a policy that [appropriately] responds to that risk").

85. *See* SOLOVE & HARTZOG, *supra* note 13, at 53–54 ("Enforcing after a breach is often the worst time to bring an enforcement action. . . . Organizations that suffer breaches are often already engaging in soul-searching and exploring how to improve in the future. . . . Additionally, the enforcement of safeguards laws does little to help compensate victims.").

86. *Id.* at 53.

87. *See infra* Part I.C.2 (discussing the Article III standing issues of breach litigation).

88. *See infra* Part I.C.2 (discussing the unlikelihood that litigation serves to motivate entities to bolster their security standards).

89. Bambauer, *supra* note 16, at 682.

90. *See supra* notes 82, 86 and accompanying text.

2. Procedural Challenges

In addition to the critical timing issue, privacy and security laws also face substantial procedural challenges. These challenges are most effectively analyzed in two categories: public enforcement and private enforcement.[91] Public enforcement is enforcement by a governmental regulator, and typically includes consent decrees, notification laws, and security safeguard laws.[92] Private enforcement occurs through litigation, accessible either by means of a statutory private right of action or under common law.[93]

There are multiple issues with public enforcement. For one, as alluded to above,[94] "there is no comprehensive federal regulatory scheme governing data breaches," but rather a patchwork of laws enforced by different agencies or sub-agencies attempting to regulate within their respective jurisdictions without much standardization.[95] The FTC is the only federal body that

91. *See* Ormerod, *supra* note 28, at 281 ("The vast majority of laws have one of two enforcement structures: either the law is exclusively enforced by one or more governmental regulators, or the law authorizes private individuals to enforce it.").

92. *See supra* notes 71–73 and accompanying text (discussing public enforcement at various levels including state agency enforcement of breach notifications and security standards at the state level and the FTC's power to prohibit unfair and deceptive practices at the federal level).

93. *See* Ormerod, *supra* note 28, at 292–302 (showcasing examples of private enforcement through litigation by way of both statutory rights of action and common law). Some federal data security laws like the Fair Credit Reporting Act (FCRA) contain private rights of action. *See, e.g.*, 15 U.S.C. § 1681(a) (including language indicating a private right of action); *see also* Ormerod, *supra* note 28, at 292–93 ("The FCRA . . . also provides for a private right of action."). In addition, many data breach victims seek redress for data breach harms and aim to supplement statutory enforcement with common law claims, including negligence, torts, and breach of contract. This need for common law supplementation could stem from the fact that the ability to litigate statutory private rights of action has been limited in several ways. *See* Ormerod, *supra* note 28, at 293–94 (discussing how the Supreme Court has limited the abilities of private citizens to litigate statutorily-conferred rights through obstacles like adhesion contracts, Article III standing issues, and class action certification); *see also* Romanosky et al., *supra* note 5, at 100 (discussing how many of the data breach cases analyzed in the article had a common law tort as their cause of action).

94. *See supra* notes 66–68 and accompanying text (discussing the patchwork federal regulatory scheme resulting from an "innovation-and-response" pattern of legislating).

95. Rabin, *supra* note 34, at 323.

has the ability to regulate data security across sectors, but it must do so under its section five power to regulate "unfair or deceptive" acts.[96] This language limits the FTC's reach to only breaches that occur because of "a material statement or omission that is likely to mislead consumers who are acting reasonably under the circumstances" (deceptive),[97] or when injury from a breach is "substantial, lacks offsetting benefits, and cannot be easily avoided by consumers" (unfair).[98] These limitations leave many major breaches outside the domain of federal enforcement.[99]

Furthermore, the typical enforcement process culminates in a fairly toothless "consent decree": a negotiated set of actions and steps that a company must take to avoid further trial and negative publicity.[100] One strong criticism of consent decrees is that, while theoretically promising, they are often enforced exclusively based on the company's own representations and subject only to "third-party" audits, which are typically conducted by other data-controlling entities with their own incentives to minimize security standards as much as possible.[101] Finally, even if the substance and outcome of public enforcement actions were strong, agencies simply do not have the capacity—personnel-

96. 15 U.S.C. § 45(a)(1); *see also* Rabin, *supra* note 34, at 323 ("The FTC is the only body that truly stretches across industries in its ability to regulate . . . ."); SWIRE & KENNEDY-MAYO, *supra* note 73, at 48–54 (discussing what the FTC's enforcement of "deceptive trade practices" and "unfair trade practices" has looked like).

97. SWIRE & KENNEDY-MAYO, *supra* note 73, at 48 (defining a "deceptive" practice).

98. *Id.* at 50 (defining an "unfair" practice). Courts have held, however, that FTC orders requiring an entity to implement a comprehensive security program are unenforceable. *Id.* at 51 (citing Kirk Nahra, *Takeaways from the 11th Circuit* FTC vs. LabMD *Decision*, IAPP (June 7, 2018), https://iapp.org/news/a/takeaways-from-the-11th-circuit-ftc-vs-labmd-decision [https://perma.cc/3VXQ-4GPN]). This suggests that, even though the FTC is the only federal organization with an omni-sectoral enforcement reach regarding data breaches, its authority to actually enforce a security remedy is, at best, questionable.

99. *See id.* at 51 (discussing how *LabMD, Inc. v. Fed. Trade Comm'n*, 678 F. App'x 816 (2016), "bring[s] into question the FTC's authority" to enforce the implementation of more stringent security standards).

100. *Id.* at 46–47.

101. Ormerod, *supra* note 28, at 291.

wise or budget-wise—to effectively bring sufficient enforcement actions to deter poor security practices.[102]

Private enforcement typically fares no better, facing three major challenges: adhesion contracts, Article III standing, and class certification.[103] With regard to adhesion contracts,[104] many data-collecting entities have users, before using their services and products, agree to arbitration and terms of use that preempt any successful litigation attempts.[105] The Supreme Court has held that the Federal Arbitration Act (FAA) applies broadly and preempts state laws in such a way that companies may effectively "immunize" themselves against litigation by compelling arbitration within their terms of service.[106] The implication of this broad policy in favor of arbitration is that, because data security and privacy claims are difficult to pursue in arbitration and large arbitration costs often fall on the plaintiff, the clauses effectively discourage breach victims from pursuing a remedy.[107]

In addition to arbitration clauses, many of these terms-of-service adhesion contracts contain notice-and-waiver mechanisms "squirreled away deep inside a thicket of legal jargon" such that entities easily defeat privacy or security claims by pointing to the users' consent to the entities' sharing of their

---

102. *See id.* at 282–87 (discussing at length the political and budgetary reasons for the dearth of enforcement actions).

103. *See id.* at 294 (explaining how these three challenges form a "complex web of obstacles that make private enforcement infeasible or impossible").

104. An adhesion contract is a "standardized contract offered on a 'take it or leave it' basis and under such conditions that a consumer cannot obtain the desired . . . service except by acquiescing in the form contract." Hosp. Auth. of Hous. Cnty. v. Bohannon, 611 S.E.2d 663, 666 (Ga. Ct. App. 2005) (quoting Walton Elec. Membership Corp. v. Snyder, 487 S.E.2d 613, 617 n.6 (Ga. Ct. App. 1997)). Such contracts are generally permissible, though courts may limit their application or refuse to enforce a term if it is unconscionable. *See* RESTATEMENT (SECOND) OF CONTRACTS § 208 cmt. a (AM. L. INST. 1981).

105. *See* Ormerod, *supra* note 28, at 294–98 (delineating the various ways that adhesion contracts negate the power of private rights of action).

106. *Id.* at 295–96 (citing AT&T Mobility LLC v. Concepcion, 563 U.S. 333, 340 (2011) (holding that the FAA preempted a California law that held most class waivers in consumer arbitration agreements unconscionable)).

107. *See id.* at 294–96 (discussing the issues with enforcing arbitration claims in privacy cases). It follows that, because data-controlling entities may use arbitration clauses as a shield post-breach against breach victims seeking remedies, they are less incentivized to bolster data security practices.

personal information.[108] Adhesion contracts thus pose a huge barrier to breach victims hoping to recover through litigation.

Even without such adhesion contracts, the intangibility of privacy harms poses an often insurmountable hurdle to breach plaintiffs.[109] In cases regarding data-controlling entities' handling of consumers' personal data, the Supreme Court has limited Article III standing in federal court to cases where harm is "concrete and particularized."[110] Consequently, the vast majority of post-breach privacy and security claims are dismissed early in the litigation process because courts find that the harms from having one's data exposed are, at least at first, only emotional or psychological, rather than physical, monetary, or reputational.[111]

Plaintiffs seeking to sidestep Article III standing by litigating in state court encounter similar barriers, as state courts often require a plaintiff to prove that the defendant's actions caused them harm.[112] State courts consistently opt not to

---

108. *See id.* at 297–98 (citing Ginwright v. Exeter Fin. Corp., 280 F. Supp. 3d 674, 681–90 (D. Md. 2017) (declining to certify a class on the grounds that users provided their consent)).

109. *See id.* at 299 (noting that many privacy laws that employ private rights of action are adversely affected by the Supreme Court's Article III standing doctrine); *see also* SOLOVE & HARTZOG, *supra* note 13, at 55 ("Courts seem so quick to dismiss claims of anxiety over a data breach that they ignore many other areas of law where anxiety alone is recognized as a cognizable harm.").

110. *See, e.g.*, TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2203 (2021). Courts typically recognize "concrete and particularized" harms to be physical harms, monetary harms, reputational harms, or explicit constitutional harms, such as infringement of free speech. *Id.* at 2204. Other "intangible" harms are less likely to confer standing to a plaintiff. *Id.* Article III standing is essentially the ability for plaintiffs to bring a case. *See, e.g.*, *id.* at 2205 (discussing how Article III standing affects whether a case can be heard by a federal court).

111. *See id.* at 2211 (stating that a "risk of future harm" was insufficient to confer standing); Ormerod, *supra* note 28, at 301–02 (discussing the implications of *TransUnion*).

112. *See, e.g.*, Maglio v. Advoc. Health & Hosps. Corp., 40 N.E.3d 746, 754 (Ill. App. Ct. 2015) (finding that, absent actual harms, the "increased risk" of identity theft or fraud due to data breach was "insufficient to confer standing"); Petta v. Christie Bus. Holding Co., P.C., 230 N.E.3d 162, 169 (Ill. App. Ct. 2023) ("[Plaintiff's] claims of an 'increased risk of identity theft' and her damages of 'time and effort' in monitoring and combating potential identity theft are simply too speculative and not imminent so as to confer standing."), *petition for leave to appeal allowed*, 232 N.E.3d 25 (unpublished table decision) (Ill. 2024); Manning v. Pioneer Sav. Bank, 55 N.Y.S.3d 587, 593 (N.Y. Sup. Ct. 2016) (finding that allegations of "potential exposure of their personal information that has

recognize harms from data breaches, however, such as anxiety and increased risk of identity theft or fraud.[113] Like federal courts, many state courts find "[a] mere increased risk of identity theft is not enough [to create standing]."[114]

Lastly, even if a plaintiff overcomes the adhesion contracts and standing hurdles, class certification is often the death knell for data breach claims in federal courts.[115] Because data breaches often affect large classes of people whose individual monetary damages are outweighed by the financial burden of pursuing litigation, class actions are often the only viable means to pursue a remedy through litigation.[116] However, trends suggest that class certification in data breach cases is limited.[117] In many data breach cases, courts will deny class certifications on predominance grounds under Rule 23(b)(3) of the Federal Rules of Civil Procedure because "common questions of liability, causation, and damages do not predominate over individualized determinations."[118] That is, courts frequently do not allow breach

---

increased their risk of identity theft . . . are too remote and not sufficient enough to confer standing"). For further discussion of state courts that have denied standing in data breach litigation, see Mitchell J. Surface, *Civil Procedure—Article III Cause-in-Fact Standing: Do Data Breach Victims Have Standing Before Compromised Data Is Misused?*, 43 AM. J. TRIAL ADVOC. 503, 509–11 (2020).

113. *See supra* note 112 and accompanying text (distinguishing between increased risk and actual harms); *see also* Solove & Citron, *supra* note 21, at 767–73 (noting the history of courts recognizing intangible harms despite a hesitancy to do so in data breach cases); *id.* at 771 ("Courts do not distinguish these cases; they simply do not mention them, as if those cases did not exist as precedent.").

114. Flores v. Aon Corp., No. 1-23-0140, 2023 WL 6333957, at *3 (Ill. App. Ct. 2023); *cf. supra* note 112 and accompanying text (describing cases where plaintiffs failed to allege actual harms); *TransUnion*, 141 S. Ct. at 2203–07 (discussing the concrete-harm requirement for Article III standing).

115. *See* Ormerod, *supra* note 28, at 303–06 (describing numerous cases where class certification has doomed data breach litigation).

116. *See id.* at 302 ("[L]ow-dollar statutory damage awards [in privacy laws] are only feasible to pursue in a class posture . . . .").

117. *See* Rabin, *supra* note 34, at 335–36 n.145 (finding that courts tend to only grant class certification under the narrow circumstances where either the cause of action falls under a federal statute or the parties have reached a settlement agreement); *see also id.* at 336 n.145 ("Only in the rare case will a class be able to show that common injuries predominate, as the range of injuries [from a data breach] is often quite wide."); FED. R. CIV. P. 23(b)(3) ("A class action may be maintained . . . if: . . . the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members . . . .").

118. Rabin, *supra* note 34, at 336 n.145.

victims to bring a case as a class because breaches affect victims to varying degrees and in varying ways.[119] Thus, class certification barriers undercut the efficacy of private litigation as a legal strategy for deterring and remedying data breaches.

In summary, the timing of breach enforcement and the procedural challenges of pursuing enforcement render the current regime of data security law inadequate to properly prevent data breaches. The long-shot odds of private enforcement give data-collecting entities perverse incentives to ignore or under-monitor security standards because they view the odds of successful actions against them as minimal.[120] Additionally, the irregularity of public enforcement is "insufficient to create a realistic threat of costs to press data controllers to take proper security measures."[121] Scholars, aware of the inadequacy of the current regime, have proposed solutions to address or sidestep some of these concerns. The next Section outlines some of the more popular proposals and expresses concerns with each proposal.

D. MODERN PROPOSALS: CREATIVE SOLUTIONS WITH THE USUAL SHORTCOMINGS

Since the dawn of the "Age of the Data Breach" in 2005, there has been no shortage of proposals to rework the privacy and security law landscape, from common law reform to vast statutory schemes.[122] This Section analyzes these proposals, starting with a common tort reform proposal, then common statutory proposals.

1. Tort Reform and "New Fiduciaries"

Tort reform discussions surrounding data breaches are particularly popular among legal scholars despite courts' apparent

---

119. *See* Ormerod, *supra* note 28, at 304 ("The same injury, however, 'does not mean merely that they have all suffered a violation of the same provision of law.' Instead, the class's 'claims must depend upon a common contention . . . which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke.'" (quoting Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 349 (2011))).

120. *See* SOLOVE & HARTZOG, *supra* note 13, at 52 ("[T]here are far too many incentives for companies to implement these standards in a minimal check-the-box manner.").

121. Bambauer, *supra* note 16, at 682.

122. *See* discussion *infra* Part I.D.1 (discussing tort reform proposals); discussion *infra* Part I.D.2 (discussing statutory reform proposals).

unwillingness to budge beyond a very specific and limited recognition of harm from data breaches.[123] One creative and popular proposal is the establishment of "Information Fiduciaries."[124] This proposal suggests that relationships between data-collecting entities and data subjects should be treated as fiduciary relationships, where the data-collecting entity has a heightened duty to protect data subjects' personal information.[125] Proponents of this idea suggest that such treatment would clarify the relevant duty and thus make litigation easier to pursue.[126]

Despite its creativity, critics quickly noted that this proposal raises more questions than it answers, particularly regarding conflicting fiduciary duties between shareholders and data subjects.[127] For one, states have statutorily reinforced the conventional view that traditional corporations may not consider non-stockholder constituencies, such as data subjects, in their

123. *See supra* notes 110–14 and accompanying text (outlining the difficulties data breach victims have in proving actual harms).

124. *See* Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 186–94 (2020) (advocating for the concept of information fiduciaries); Solow-Niederman, *supra* note 21, at 614 (finding the fiduciary-like relationship argument more reliable than statutory claims for protecting consumer data); *cf.* Khan & Pozen, *supra* note 21, at 521–28 (identifying issues related to imposing fiduciary duties on online platforms). Other proposals include strict liability enforcement by federal agencies and creating statutory harm with private rights of action. *See* James C. Cooper & Bruce H. Kobayashi, *Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem*, 28 MICH. TECH. L. REV. 257, 287–96 (2022) (arguing that strict liability is more effective than negligence for data security regulation); Ignacio Cofone, *Beyond Data Ownership*, 43 CARDOZO L. REV. 501, 542 (2021) (explaining that liability, although taking away data subject control, allows consumers to efficiently remedy harm in data breaches). While these proposals are also creative and address some challenges of privacy law in general, they fail to meaningfully address the specific challenges of breach prevention discussed above and are thus largely outside the scope of this Note. *See supra* Part I.C (discussing the historical, procedural, and substantive hurdles to successful breach deterrence and enforcement).

125. *See* Scholz, *supra* note 124, at 145 (explaining a possible mechanism for the institution of fiduciary relationships between consumers and data-collecting entities).

126. *See id.* at 195 (noting that the implementation of a fiduciary relationship would make data privacy cases more difficult to dismiss); Solow-Niederman, *supra* note 21, at 629–33 (suggesting the same).

127. *See* Khan & Pozen, *supra* note 21, at 504 (criticizing the feasibility of information fiduciary theory).

decision-making.[128] Typically, in for-profit companies, the board and officers owe a fiduciary duty only to the company's shareholders to maximize profit, without consideration of non-shareholder constituencies.[129] Imposing an additional duty to data subjects may directly conflict with the duty to shareholders in cases where acting in the best interest of data security is significantly opposed to the pursuit of profit.[130] While there are professions, such as doctors or lawyers, where some level of conflicting fiduciary duties may exist, the case of potential conflicts between owners and end users of data-handling entities go so much to the "core of the firms' business" that mitigating strategies are infeasible.[131] Thus, a fiduciary duty to data users could expose companies to situations where acting in the best interest of the data subjects conflicts with their profit-maximizing duty, causing headaches for boards, investors, and courts.[132]

2. Statutory Proposals: The GDPR, CCPA, ADPPA, and APRA

Recent statutes and statutory proposals similarly miss the mark when addressing the challenges of data security. Some have resulted in vast regulatory schemes, such as the European Union's General Data Protection Regulation (GDPR) of 2016, which established expansive public and private enforcement of data breach laws for Europeans.[133] Many U.S. states tried to model their own statutes after the GDPR to varying degrees, suggesting a "revolution" in American privacy and security law.[134] However, scholars note that the "revolution is only a façade," with some even condemning the new laws as "insipid,

128. *See id.* (noting that Delaware fiduciary law does not allow traditional corporations to consider potentially contradictory interests in their decision-making).

129. *See id.* (distinguishing these traditional companies from public benefit corporations).

130. This is especially true in the case of companies whose primary trade is the buying and selling of consumers' personal data for the purpose of ad sales. *See, e.g.*, *Data Brokers,* EPIC (Mar. 7, 2024), https://epic.org/issues/consumer-privacy/data-brokers [https://perma.cc/NFG7-28HS] (describing the lack of oversight on the data broker industry).

131. Khan & Pozen, *supra* note 21, at 507.

132. *See id.* (discussing the possible conflicts that may arise with information fiduciary obligations, such as the conflict between limiting data exposure versus data's marketing benefits).

133. *See generally* Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

134. *See* Ormerod, *supra* note 28, at 268–69.

porous, and ineffective."[135] The California Consumer Privacy Act (CCPA), later the California Privacy Rights Act (CPRA), and similar laws enacted in Virginia, Colorado, and Utah all impose massive obligations on data-controlling entities through requiring data-use disclosures and requiring notifications after breaches.[136] The proposed American Data Privacy and Protection Act (ADPPA) and subsequent American Privacy Rights Act (APRA) similarly focus on data rights, disclosures, and notifications.[137]

As ambitious as these statutes and proposals may be, they employ the same two methods of enforcement—public enforcement and private rights of action—that have proven inadequate in addressing breaches.[138] Further, a comprehensive research study has suggested that breach notification laws do not actually deter data breaches or promote the development of a market for data security firms.[139] Even in cases where the duty on the data handling is clearly defined to prevent breaches (as in the proposed texts of the ADPPA and APRA),[140] proposals falter in their use of traditional enforcement mechanisms that have proven insufficient in deterring breaches.[141]

The approach to data security enforcement mechanisms in sum has been largely ineffective. More recently, data security law has been hyper-focused on the occurrence of a breach as a focal point for enforcement, which is too late to be effective in preventing breaches. Further, key issues burden the effectiveness of data security law—specifically, agency underenforcement, adhesion contracts, standing, and class certification.

---

135. *Id.* at 270.

136. *See id.* at 277–79 (discussing flaws in state privacy laws).

137. *See* H.R. REP. NO. 117-669, at 1 (2022) (providing a draft of the ADPPA's text); CHRIS D. LINEBAUGH ET AL., CONG. RSCH. SERV., LSB11161, THE AMERICAN PRIVACY RIGHTS ACT 2–4 (2024) (summarizing the APRA).

138. *See supra* Part I.C (arguing that public enforcement and private rights of action do not sufficiently protect consumers from data breaches).

139. *See* Greenwood & Vaaler, *supra* note 71, at 26 ("From 2005–2019, [breach notification laws] significantly reduced neither data breach counts nor magnitudes.").

140. H.R. REP. NO. 117-669, at 10–11 (2022) (outlining the duty of entities in handling user data based on a reasonableness standard as determined by the FTC); LINEBAUGH ET. AL., *supra* note 137, at 2 (discussing the rights and obligations of covered entities under the APRA).

141. *See supra* Part I.C (discussing the insufficiency of public law surrounding data breaches and procedural barriers to those affected by data breaches).

Recent scholarship, however, suggests that an alternative enforcement mechanism may offer a solution.[142] Part II of this Note examines qui tam as a tool in American jurisprudence that could help bolster the data security legal regime through enforcement before the breach.

II. QUI TAM REVIVAL: AN OLD MECHANISM WITH NEW ASPIRATIONS

Qui tam is a civil action whereby an individual, called a "relator," sues on behalf of the government to vindicate a public right.[143] Depending on how the action is statutorily enacted, the relator may either bring the suit as an agent of the government or as an assignee of the government's claims.[144] If the suit is successfully litigated or results in a settlement, the relator receives a share of the proceeds.[145] Originating in thirteenth-century England as a common-law action,[146] "qui tam" is short for a longer Latin phrase that means "who as well for the king as for himself sues in this matter."[147] Despite some historical uses of qui tam provisions being criticized for incentivizing over-litigious plaintiffs and their attorneys,[148] qui tam has been called for, authorized, and praised by legislatures where enforcement

142. *See generally, e.g.*, Ormerod, *supra* note 28 (arguing that qui tam would be a viable means to better effectuate the enforcement of privacy violations).

143. *See* BRYAN A. GARNER, GARNER'S DICTIONARY OF LEGAL USAGE 745 (3d ed. 2011) (defining qui tam as "an action under a statute that allows a private person to sue for a penalty, part of which the government or some specified public institution will receive"); CHARLES DOYLE, CONG. RSCH. SERV., R40785, QUI TAM: THE FALSE CLAIMS ACT AND RELATED FEDERAL STATUTES 1 (2021) (defining qui tam as "the process whereby an individual sues or prosecutes in the name of the government and shares in the proceeds of any successful litigation or settlement"); United States *ex rel.* Polansky v. Exec. Health Res., Inc., 143 S. Ct. 1720, 1727 (2023) ("Those suits are 'brought in the name of the Government.'" (quoting 31 U.S.C. § 3730(b)(1))).

144. *See infra* Part II.B.

145. *See* DOYLE, *supra* note 143 (discussing the mechanisms of qui tam).

146. *See* Ormerod, *supra* note 28, at 308 (citing GARNER, *supra* note 143, at 745).

147. The full phrase is "qui tam pro domino rege quam pro se ipso in hac parte sequitur." United States v. Molina Healthcare of Ill. Inc., 17 F.4th 732, 739 (2021) (citing *Qui tam*, BLACK'S LAW DICTIONARY (10th ed. 2014)).

148. Such plaintiff's attorneys have been derided as "'viperous vermin' and parasites." DOYLE, *supra* note 143, at 1 (footnote omitted).

of a given law is "beyond the unaided capacity or interest of authorized law enforcement officials."[149]

At present, there is no common-law right to bring a qui tam action in the United States—that is, Congress must explicitly create qui tam actions.[150] While qui tam statutes and lawsuits were fairly common in colonial America and the early days of the United States, they have largely fallen into disuse.[151] Today, there are only two federal statutes with active qui tam provisions: the False Claims Act (FCA) and an American Indian protection law.[152] The FCA provision is a prominent example of a federal law that authorizes qui tam enforcement, and is instructive to legislatures who may seek to effectively employ qui tam in new legislative proposals.[153]

This Part surveys qui tam in the United States. Part II.A dives into the FCA before highlighting its recent application in data security cases. Part II.B surveys the recent resurgence of qui tam in newer proposals, concluding with an outline of a recent proposal that advocates for qui tam enforcement in privacy laws.[154]

A. THE DEVELOPMENT OF QUI TAM IN THE FALSE CLAIMS ACT

The FCA "imposes civil liability on any person who presents false or fraudulent claims for payment to the Federal Government" and is enforceable through its qui tam provision.[155] An

149. *Id.*

150. *See* Ormerod, *supra* note 28, at 308 (citing United Seniors Ass'n v. Philip Morris USA, 500 F.3d 19, 23 (1st Cir. 2007)); DOYLE, *supra* note 143, at 4–5 (stating that courts have "refused to recognize any implicit authority to bring a qui tam action").

151. *See* DOYLE, *supra* note 143, at 4 (noting that qui tam statutes "had largely fallen into disuse" by "the turn of the twentieth century").

152. *See id.* (explaining that two additional contemporary federal qui tam statutes—a separate American Indian protection law and the Patent Act—were amended or had their qui tam actions replaced (citing Vermont Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 768–69 n.1 (2000))).

153. *See* Ormerod, *supra* note 28, at 308–09 ("[T]he False Claims Act (FCA) is the most prominent example of a federal law that authorizes qui tam enforcement."); DOYLE, *supra* note 143, at 4 ("Of the two survivors, the False Claims provision is by far the more often invoked.").

154. *See* Ormerod, *supra* note 28, at 318 (proposing that legislation should be drafted to enable a privacy qui tam).

155. United States *ex rel.* Polansky v. Exec. Health Res., Inc., 143 S. Ct. 1720, 1726 (2023). The elements of an FCA claim for legal analysis generally

FCA relator typically brings a suit through the qui tam provision as a partial assignee of the Government's claims.[156] If the suit is successful, the defendant is liable for a civil penalty of up to $10,000 plus three times the amount of damages sustained by the Government as a result of the defendant's acts,[157] and the relator may receive up to thirty percent of that amount.[158]

Additionally, qui tam relators of FCA actions are subject to special procedural restrictions. For one, the relator must file its complaint under seal, as well as deliver a copy of the complaint along with supporting material evidence to the Government.[159] The Government then has sixty days to decide whether to intervene and proceed with the action.[160] If the Government decides to intervene within that period, it takes the primary role in pursuing the action, though the relator may continue as a party in a lesser role.[161] If the Government declines to intervene, only then does the relator "have the right to conduct the action."[162] Even if the Government declines to intervene, it has continuing rights in the action, including the majority of the recovery, the

include: "(1) a false statement or fraudulent course of conduct, (2) made with the scienter, (3) that was material, causing (4) the government to pay out money or forfeit moneys due." Jack Burns, *Data Mining for Qui Tam False Claims Act Suits: Business Opportunity for the Technology Age, or Doomed Goose Chase?*, 22 TUL. J. TECH. & INTELL. PROP. 1, 6 (2020) (quoting United States *ex rel.* Campie v. Gilead Scis., Inc., 862 F.3d 890, 902 (9th Cir. 2017)).

156. This role is as opposed to that of an agent. *See infra* Part II.B (discussing the agency and assignment theories of qui tam relators).

157. Ormerod, *supra* note 28, at 309 (quoting 31 U.S.C. § 3729(a)(1)(G) (2018)).

158. *Polansky*, 143 S. Ct. at 1727 (citing 31 U.S.C. § 3730(d)(1)–(2)). The relator is entitled to 15–25% of the award if the Government intervenes, and 25–30% if it does not. Ormerod, *supra* note 28, at 309 (quoting 31 U.S.C. § 3730(d)(1)–(2) (2018)).

159. *Polansky*, 143 S. Ct. at 1723 (quoting 31 U.S.C. § 3730(b)(2)); *see also* Ormerod, *supra* note 28, at 309 (describing the FCA's qui tam requirements).

160. *Polansky*, 143 S. Ct. at 1723 (citing 31 U.S.C. § 3730(b)(2)–(3)). This sixty-day period may also be extended for "good cause," and often is. *Id.*

161. *Id.* at 1728. In the lesser role, "the relator retains three rights: to continue as a party in the action, to a hearing before voluntary dismissal, and to a court determination of reasonableness before settlement." Ormerod, *supra* note 28, at 309 (citing 31 U.S.C. § 3730(c)(1)–(2)(B)).

162. *Polansky*, 143 S. Ct. at 1728 (citing 31 U.S.C. § 3730(b)(4)(B)).

power to intervene after the seal period ends, and the ability to dismiss a qui tam action over the relator's objection.[163]

The FCA's qui tam provision is worthy of discussion here not only because of its prominence, but also because of its resilience in the face of constitutional challenges.[164] Recent clarity from the Supreme Court suggests that its current form and use may serve as a model for crafting qui tam provisions in other statutes.[165] This Section proceeds to explore this potential by first providing an overview of the history and development of the FCA before turning to its modern applications and reaffirmed constitutionality. This Section concludes with an analysis of the Civil Cyber-Fraud Initiative—a recent application of the FCA in data security that serves as a proof-of-concept for more expansive qui tam security laws.

1. The History of the FCA and its Qui Tam Provision

The FCA originated during the Civil War as the Act of March 2, 1863, to combat fraud in the procurement of Civil War defense contracts.[166] This original version of the law prohibited fraud against the federal government, including the presentation of false claims, vouchers, or oaths; forged signatures; theft; embezzlement; and conspiracy.[167] Offenders faced a criminal penalty of one to five years imprisonment and a fine between

163. *Id.* at 1728–29, 1733–34. The last of the three continuing rights listed above were the subject of a circuit split up until the Court in *Polansky* resolved the split in June 2023. *See id.*

164. *See infra* Part II.A.2 (discussing the ability of qui tam to reach Article III requirements). *But see supra* note 183 (discussing a September 30, 2024 United States district court case holding that the FCA's qui tam provision violates the Appointments Clause under Article II of the Constitution).

165. *See* DOYLE, *supra* note 143, at 35–44 (discussing recent Supreme Court cases finding the False Claims Act's qui tam provision constitutional); Vermont Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 774 (2000) (upholding that injury-in-fact sustained by the United States Government is sufficient to confer Article III standing in qui tam actions); *see also Polansky*, 143 S. Ct. at 1728–30 (clarifying the roles that the Government may have in qui tam actions).

166. DOYLE, *supra* note 143, at 6 (citing Act of March 2, 1863, ch. 67, 12 Stat. 696); Beverly Cohen, *KABOOM! The Explosion of Qui Tam False Claims Under the Health Reform Law*, 116 PENN ST. L. REV. 77, 80 (2011) ("The Act was adopted during the Civil War to combat fraud in war procurement contracts . . . .").

167. DOYLE, *supra* note 143, at 6 (citing Act of March 2, 1863, ch. 67, 12 Stat. 696).

$1,000 and $5,000, as well as civil liability of $2,000, double the amount of damages sustained by the Government, and costs.[168] Qui tam relators were entitled to half of the penalty recovered and costs if successful.[169]

The qui tam provision remained essentially unchanged until 1943, when the attorney general urged Congress to repeal the provision, in part because the actions are based on already-available information.[170] In response, Congress passed an amendment that: required relators to provide evidence for the basis of their litigation and allow the Government sixty days to intervene; precluded qui tam suits based on information already available to the Government; and reduced the relator's share to a maximum of 10% if the Government did intervene and 25% if it did not.[171]

In response to evidence of extensive fraud against the United States Government, Congress again updated the FCA in 1986 to reinvigorate qui tam procedures.[172] Specifically, the update added protection for whistleblowers, increased sanctions, and increased the maximum award available to relators.[173] Amendments in 2009 and 2010 further empowered relators to aid in fraud detection and enforcement.[174] As of this Note's publication, the FCA has remained largely the same since these

---

168. *Id.*

169. *Id.*

170. *See id.* at 7 (expressing the futility of whistleblowers when the information they provide is already publicly available (first citing S. REP. NO. 77-1708, at 1–2 (1942); and then citing H.R. REP. NO. 78-263, at 1–2 (1943))).

171. *Id.* at 7–8 (citing An Act to Limit Private Suits for Penalties and Damages Arising Out of Frauds Against the United States, Pub. L. No. 78-213, 57 Stat. 608, 608–09 (1946)).

172. *Id.* at 8 n.57 ("The Department of Justice has estimated fraud as draining 1 to 10 percent of the entire Federal budget." (citing S. REP. NO. 99-345, at 2–3 (1986))).

173. *Id.* at 8–9 (citing 31 U.S.C. §§ 3729–30 (1988)). In addition, the update clarified the level of knowledge required for a violation (declaring that specific intent was unnecessary), established a preponderance-of-evidence burden of proof, declared that states could act as relators, and expanded the statute of limitations. *Id.*

174. *Id.* at 9–10; *see also* Cohen, *supra* note 166, at 89 ("[B]y limiting what constitutes public disclosure and by deleting the stringent 'direct knowledge' requirement of the original source rule, Congress dramatically expanded the ability of relators to maintain [FCA] qui tam lawsuits.").

updates.[175] While the FCA allows an action to be commenced either by the U.S. Attorney General or by qui tam, the vast majority of litigation is brought through its qui tam mechanism.[176]

2. Constitutional Challenges to the FCA

Despite the unorthodoxy of qui tam as an enforcement mechanism in the FCA, its legitimacy has withstood significant constitutional challenges under Article III.[177] The Supreme Court dictated in 2000, and again in 2023, that, even though individual relators initially bring the FCA suit and receive a nontrivial portion of the damages, Article III standing is nonetheless satisfied—regardless of whether the relator acts merely as an "agent" of the Government, bringing the suit entirely on its behalf, or as an "assignee" of the Government, maintaining some interest in the suit.[178] In the agency model, this is because the injury asserted is exclusively that of the Government.[179] Whether the governmental injury be an "injury to its sovereignty arising from [the] violation of [the statute]" or "the proprietary injury resulting [therefrom]," it is sufficient for standing purposes that the relator-agent's recovery is "simply the fee . . . for filing and/or prosecuting a successful action on behalf of the Government"—standing is satisfied by the Government's position in the suit.[180] Similarly, in the assignment model, the Court held that adequate standing is conferred to the relator-assignee by

175. *See* DOYLE, *supra* note 143, at 10 (noting no changes to the FCA after the 2010 amendments).

176. *See* Ormerod, *supra* note 28, at 309 (noting the two ways to commence an FCA action); 31 U.S.C. § 3730(a)–(b); David Freeman Engstrom, *Private Enforcement's Pathways: Lessons from Qui Tam Litigation*, 114 COLUM. L. REV. 1913, 1944 n.103 (2014) (citing that, in 2013, qui tam suits outnumbered government-initiated matters 700 to 93).

177. *See, e.g.*, Ormerod, *supra* note 28, at 310 (noting the Supreme Court's recent decision on FCA relator standing).

178. *See* Vermont Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 771–75 (2000) (explaining that standing exists under both the agency and assignment models, as supported by the lengthy histories of the actions); *see also* United States *ex rel.* Polansky v. Exec. Health Res., Inc., 143 S. Ct. 1720, 1727–28 (2023) (coming to similar conclusions as *Stevens* on standing). See Part II.B for further discussion of the agency and assignment relator models.

179. *See Stevens*, 529 U.S. at 771–72 (describing the agency model).

180. *Id.; see also Polansky*, 143 S. Ct. at 1727 ("A *qui tam* suit, this Court has explained, alleges both an 'injury to the [Government's] sovereignty arising from violation of its laws' and an injury to its 'proprietary [interests] resulting from [a] fraud.'" (alterations in original) (quoting *Stevens*, 529 U.S. at 771)).

the Government as "effecting a partial assignment of the [assignor's] damages claim."[181] The Court thus affirmed the FCA's qui tam mechanism as valid and effective for Article III standing.

A recently more successful line of constitutional criticism to the FCA's qui tam provision is through Article II, specifically regarding the Appointments Clause.[182] On September 30, 2024, the United States District Court for the Middle District of Florida went so far as to hold the FCA's qui tam provision unconstitutional on Appointments Clause grounds.[183] To do so, the court applied the Supreme Court's "officer" test and held that an FCA relator is an officer of the United States because "she [(1)] 'exercis[es] significant authority pursuant to the laws of the United States,' . . . and [(2)] 'occup[ies] a "continuing" position established by law.'"[184] The court reasoned that the power to "'conduct[] civil litigation in the courts of the United States for vindicating public rights'" satisfies the significant authority branch of the officer test.[185] The court then analogized relators to bank receivers and special prosecutors, stating that even those appointed to a single term with an expiration may satisfy the continuing position branch of the officer test.[186]

The case is on appeal at the Eleventh Circuit as of this Note's publication, with Appellant briefs due on January 8, 2025.[187] While the Eleventh Circuit has not dealt with the

181. *See Stevens*, 529 U.S. at 773 (describing the assignment model).

182. *See* U.S. CONST. art. II, § 2, cl. 2 (outlining the Appointments power). Other Article II challenges focus on the Take Care Clause and separation of powers concerns. *See id.* art. II, § 3, cl. 1 (outlining the Take Care power); *e.g.*, *Polansky*, 143 S. Ct. at 1741 (Thomas, J., dissenting) ("There are substantial arguments that the *qui tam* device is inconsistent with Article II and that private relators may not represent the interests of the United States in litigation.").

183. United States *ex rel.* Zafirov v. Florida Med. Assocs., LLC, No. 19-cv-01236, 2024 WL 4349242, at *16, *19–20 (M.D. Fla. Sept. 30, 2024) (relying heavily on Justice Thomas's dissent in *Polansky* to hold that qui tam is unconstitutional).

184. *Id.* at *6 (first quoting Lucia v. SEC, 138 S. Ct. 2044, 2051 (2018); then quoting Buckley v. Valeo, 424 U.S. 1, 126 (1976) (per curiam); and then quoting United States v. Germaine, 99 U.S. 508, 511 (1879)).

185. *Id.* at *7 (quoting *Buckley*, 424 U.S. at 126).

186. *Id.* at *13.

187. *See* Notice of Appeal, United States *ex rel.* Zafirov v. Florida Med. Assocs., LLC, No. 24-13581 (11th Cir. Oct. 29, 2024); Extension Granted, *Zafirov*, No. 24-13581 (11th Cir. Nov. 14, 2024).

Appointments Clause issue directly, it has spoken favorably in dicta about other circuit courts' rejections of Article II challenges, noting (1) the significant amount of control the FCA qui tam provision affords the government over a qui tam suit and (2) qui tam's long history in the United States.[188] In this Author's opinion, the significant control that the government exercises over an FCA qui tam action—including its power to intervene and its power to dismiss even without intervention—differentiates the position of an FCA relator from bank receivers and special prosecutors such that no continuing position necessarily exists.[189] Nonetheless, if *Zafirov* is upheld on appeal, the Eleventh Circuit would create a circuit split with the Fourth, Fifth, Sixth, and Ninth Circuits that the Supreme Court may very well be eager to address.[190]

The *Zafirov* court also noted that alternative qui tam mechanisms exist that, in its view, likely do not violate the Appointments Clause: such as those that provide "a bounty only," i.e., those that yield total control of a qui tam lawsuit to the government upon filing.[191] Such a mechanism, *Zafirov* argues, "does not authorize the [relator] to wield power, much less the core executive power a relator exercises by litigating on behalf of the United States."[192] If *Zafirov* makes its way to the Supreme Court, it may be wise for a Congress hoping to preserve the efficacy of the FCA to have ready an amendment to its qui tam

188. *E.g.*, Yates v. Pinellas Hematology & Oncology, P.A., 21 F.4th 1288, 1312 (11th Cir. 2021) ("Precisely because of the United States' significant control over FCA qui tam actions, our sister circuits have held that they do not violate . . . Article II's Take Care Clause . . . ."); *see also id.* at 1313 ("[Q]ui tam actions were viewed as a routine enforcement mechanism in the early Republic.").

189. *See id.* at 1312 (describing "the United States' considerable authority over intervened and non-intervened qui tam actions").

190. *See supra* note 187 and accompanying text (discussing qui tam's resilience in circuit courts against Appointments Clause challenges); *see also* Ormerod, *supra* note 28, at 332 ("There are good reasons to be concerned that stringent interpretations of [Article II] are ascendant among the current Court." (first citing Seila Law LLC v. Consumer Fin. Prot. Bureau, 141 S. Ct. 2183, 2211 (2020); and then citing United States v. Arthrex, Inc., 141 S. Ct. 1970, 1972 (2021))).

191. *Zafirov*, 2024 WL 4349242, at *16–17 (citing Vermont Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 775–77 (2000)).

192. *Id.* at *17.

provision that expressly relinquishes a relator's control over the action to the government upon filing under seal.[193]

In addition to Appointments Clause Challenges, other lines of Article II criticisms include Take Care Clause challenges as well as separation of powers concerns.[194] In sum, Article II criticisms generally contend that: qui tam violates the Appointments Clause because relators "exercise significant authority" in enforcing the laws of the United States;[195] qui tam violates the Take Care Clause because it "reduc[es] the President's ability to control the prosecutorial powers" of relators and independent counsel;[196] or qui tam conflates the executive power with that of the judiciary.[197] The largest and most obvious argument against these criticisms—and the *Zafirov* holding on appeal—is qui tam's lengthy history in the United States.[198] Not only were qui tam statutes fairly common when the Constitution was drafted, but qui tam statutes were "enacted by the early Congresses, populated by the men responsible for drafting and ratifying the new Constitution," thus providing "contemporaneous and weighty evidence of the Constitution's meaning."[199] In other words, critics face a substantial barrier in trying to explain the unconstitutionality of a process which the Framers viewed as perfectly constitutional.[200]

The Fourth, Fifth, Sixth, and Ninth Circuits have also agreed in holding that qui tam in the FCA does not raise these Article II concerns, as relators have neither a "continuing and

193. *See id.* It follows that any new qui tam provisions—such as a security qui tam provision—should also expressly limit the relator's control upon filing. *See infra* note 261 and accompanying text (discussing the requirements of a security qui tam statute).

194. *See, e.g.*, United States *ex rel.* Polansky v. Exec. Health Res., Inc., 143 S. Ct. 1720, 1741 (2023) (Thomas, J., dissenting) ("There are substantial arguments that the *qui tam* device is inconsistent with Article II and that private relators may not represent the interests of the United States in litigation.").

195. *See* Ormerod, *supra* note 28 at 332 (citing United States v. Arthrex, Inc., 141 S. Ct. 1970, 1978–80 (2021)).

196. *See* DOYLE, *supra* note 143, at 44 (quoting Morrison v. Olson, 487 U.S. 654, 685 (1988)).

197. *See id.* at 44.

198. *See id.* at 3–4.

199. *Id.* at 40–41 (quoting Bowsher v. Synar, 478 U.S. 714, 723 (1986)).

200. *See id.* at 41 ("[C]ritics face the problem of explaining how a process, which the Framers did not consider unconstitutional, should now be so construed.").

formalized relationship" with the Government, nor an obligation to prosecute further qui tam cases, and thus do not limit the executive's prosecutorial powers.[201] Further, because the FCA allows the Government to intervene and dismiss qui tam suits,[202] it "affords the Executive Branch sufficient control to turn aside a Take Care Clause challenge."[203] In sum, despite recent constitutional challenges, the FCA's qui tam provision has proven resilient in most courts, though further litigation over its constitutionality under Article II seems likely.

3. Modern Enforcement and the Civil Cyber-Fraud Initiative

Backed by the Supreme Court's validations of the legitimacy of the FCA's qui tam provision, the Department of Justice (DOJ) has recently found success in advocating for its increased use.[204] In February of 2023, the DOJ noted that the FCA is of high importance in protecting government funds, stating that its "ability to protect citizens and taxpayer funds continues to benefit greatly from [qui tam relators'] actions."[205] Since the 1986 amendments, recoveries under the FCA have exceeded $72 billion.[206] In fiscal year 2022, $2.2 billion was recovered in settlements and judgments with over eighty-six percent coming from qui tam lawsuits.[207] Recent FCA suits span various sectors, including healthcare;[208] military spending and

201. *See* Ormerod, *supra* note 28, at 332 (quoting Riley v. St. Luke's Episcopal Hosp., 252 F.3d 749, 753–58 (5th Cir. 2001) (en banc)).

202. *See supra* Part II.A.1; *infra* Part III (discussing the mechanisms of the FCA and how a security qui tam statute should be closely modeled after the FCA, specifically by allowing the government power to intervene or dismiss a qui tam suit).

203. *See* DOYLE, *supra* note 143, at 45 (citing United States *ex rel.* Kelly v. Boeing Co., 9 F.3d 743, 757 (9th Cir. 1993)).

204. *See infra* notes 205–14 and accompanying text (discussing recent DOJ efforts).

205. Press Release, U.S. Dep't of Just., False Claims Act Settlements and Judgments Exceed $2 Billion in Fiscal Year 2022 (Feb. 7, 2023), https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-2-billion-fiscal-year-2022 [https://perma.cc/7Q9U-696M].

206. *Id.* (discussing FCA recoveries).

207. *Id.* (describing how, of the $1.9 billion recovered via qui tam suits, around twenty-six percent was paid out to relators).

208. This is by far the most common sector, accounting for $1.7 billion of the $2.2 billion recovered under the FCA in 2022. *Id.* Subcategories within the healthcare category include Medicaid fraud and abuse, unnecessary services

servicemember/first responder safety; COVID-19-related fraud;[209] shipping and freight; services for low-income families; and cybersecurity.[210]

In October 2021, the DOJ announced the Civil Cyber-Fraud Initiative (CCFI), highlighting a need to bolster government enforcement of data security and combat "emerging cyber threats to the security of sensitive information and critical systems."[211] Through the CCFI, the DOJ aims to use the FCA and its qui tam provision to prevent breaches involving government contractors and "improv[e] overall cybersecurity practices that will benefit the government, private users and the American public."[212] The CCFI is effectuated under the FCA through the DOJ's power to pursue those who present "false or fraudulent claim[s] for payment" to the federal government.[213] It aims to utilize the FCA's qui tam provision to hold accountable government contractors and grant recipients who "put U.S. information or systems at risk" when such entities knowingly "provid[e] deficient cybersecurity products or services," "misrepresent[] their cybersecurity practices or protocols," or "violat[e] obligations to monitor and report cybersecurity incidents and breaches."[214]

As of this Note's publication, only a handful of cases have been unsealed[215] under the CCFI, with the Government intervening for the first time in 2024.[216] This recent intervention

---

and substandard care, Medicare Advantage matters, drug pricing, and unlawful kickbacks. *Id.*

209. The government recovered $6.8 million and avoided another $1.5 million in losses related to the Paycheck Protection Program and Small Business Administration Loans. *Id.*

210. *See id.* (listing the sectors that have been subject to recent FCA lawsuits).

211. U.S. Dep't of Just., *supra* note 31 (describing the new initiative to bolster data security efforts).

212. *Id.* (detailing the goals of the CCFI).

213. *See* DOYLE, *supra* note 143, at 15.

214. U.S. Dep't of Just., *supra* note 31 (describing the purpose of the DOJ program).

215. A case is initially given to the government under seal and is unsealed to the public after the government has reviewed the case. *See supra* notes 159–63.

216. Press Release, U.S. Att'y's Off., N.D. Ga., United States Files Suit Against the Georgia Institute of Technology and Georgia Tech Research Corporation Alleging Cybersecurity Violations (Aug. 23, 2024) [hereinafter Georgia Tech], https://www.justice.gov/usao-ndga/pr/united-states-files-suit-against

indicates that the Government indeed intends to litigate cybersecurity fraud claims brought via qui tam, giving some momentum to the qui tam-effectuated CCFI.[217] Two recent cases—in one of which the Government intervened—were brought via qui tam against separate universities and allege that the universities falsely claimed to comply with all required cybersecurity standards in procuring government contracts.[218] In each case, the universities run research labs that contract with the Department of Defense and were required to attest to compliance with government-issued security standards.[219] The suits both allege that university officials submitted materially-false documents and stored sensitive information in a non-compliant manner.[220] Four other cases have settled, resulting in recovery of over $5.31

-georgia-institute-technology-and-georgia-tech [https://perma.cc/89HY-7JW6] (discussing the government's intervention in a recent qui tam action involving Georgia Tech and its alleged failures to implement cybersecurity measures required by Department of Defense contracts); Press Release, U.S. Dep't of Just., The Pennsylvania State University Agrees to Pay $1.25M to Resolve False Claims Act Allegations Relating to Non-Compliance with Contractual Cybersecurity Requirements (Oct. 22, 2024) [hereinafter Penn State], https://www.justice.gov/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating [https://perma.cc/U9EB-ZDK7] (noting the settlement of a recent case involving a Penn State laboratory that contracted with the Department of Defense). An additional high-profile FCA case regarding cybersecurity compliance was unsealed in April of 2021 and settled in July of 2022. *See* Press Release, U.S. Dep't of Just., Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts (July 8, 2022), https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity [https://perma.cc/6NBF-FE4E] ("Aerojet Rocketdyne Inc. . . . agreed to pay $9 million to resolve allegations that it violated the False Claims Act by misrepresenting its compliance with cybersecurity requirements in certain federal government contracts . . . ."); *see also* United States *ex rel.* Markus v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240 (E.D. Cal. 2019); *In re* V. Aerojet Rocketdyne Holdings, Inc., No. 15-cv-2245, 2022 U.S. Dist. LEXIS 117673 (E.D. Cal. July 1, 2022).

217. *See* Georgia Tech, *supra* note 216 (providing information on the CCFI and noting that "[t]his lawsuit is the first matter the United States has litigated as part of the [CCFI]").

218. *See id.* (noting the Government's intervention and complaint); Penn State, *supra* note 216 (noting the settlement of the lawsuit).

219. *See* Georgia Tech, *supra* note 216 (explaining the obligations of the university under its contract with the Department of Defense); Penn State, *supra* note 216 (same).

220. *See* sources cited *supra* note 219 (describing the allegations of the lawsuits).

million in damages—demonstrating the potential efficacy of qui tam enforcement to rectify substandard data security before a large-scale breach need occur.[221]

While the recent success of the CCFI in effectuating better security law is promising, the scope of the FCA is narrow in that it covers only government contractors and federal grant recipients.[222] A broader qui tam security scheme is necessary to ensure the security of large swaths of personal data held by entities that are not subject to the CCFI. Extending the FCA's spirit to broader qui tam data security enforcement would provide an incremental but crucial step in enhancing data security and preventing breaches. The next Section explores recent qui tam proposals that provide further guidance toward security qui tam before Part III turns to this Note's specific proposals.

---

221. *See generally, e.g.*, Press Release, U.S. Dep't of Just., Cooperating Federal Contractor Resolves Liability for Alleged False Claims Caused by Failure to Fully Implement Cybersecurity Controls (Sept. 5, 2023), https://www.justice.gov/opa/pr/cooperating-federal-contractor-resolves-liability-alleged-false-claims-caused-failure-fully [https://perma.cc/KMV8-JBFM] (describing a settlement agreement between the Government and Verizon for allegedly failing to satisfy cybersecurity standards in IT services provided to federal agencies, where Verizon itself provided the disclosure); Press Release, U.S. Dep't of Just., Jelly Bean Communications Design and Its Manager Settle False Claims Act Liability for Cybersecurity Failures on Florida Medicaid Enrollment Website (Mar. 14, 2023), https://www.justice.gov/opa/pr/jelly-bean-communications-design-and-its-manager-settle-false-claims-act-liability [https://perma.cc/NTB3-CF4M] (describing a settlement agreement where the relator alleges that Jelly Bean Communications Design LLC failed to secure personal information on a federally-funded website); Press Release, U.S. Dep't of Just., Medical Services Contractor Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan (Mar. 8, 2022), https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical [https://perma.cc/YUF3-AZ7Z] (describing a settlement agreement of two qui tam cases against a military contractor who allegedly failed to disclose that medical records of government employees were not stored on a secure system).

222. *See supra* notes 211–14 and accompanying text (discussing the CCFI and recent efforts surrounding the FCA).

B. "NEW" QUI TAM PROPOSALS AND RELATOR THEORIES

In the past few decades, there has been renewed interest in qui tam beyond novel applications of the FCA.[223] This Section provides an overview of two of these new proposals before discussing the distinction both proposals make between agency and assignment relator models for qui tam provisions.

In 2020, Professor Myriam Gilles and practicing attorney Gary Friedman coauthored a law review article urging the adoption of state laws with qui tam actions.[224] The article, inspired by what the authors call an "increasingly hostile" federal and judicial posture towards rights enforcement,[225] argues that qui tam provisions within state legislation may provide a solution for cash-strapped state consumer protection agencies to enforce public rights in the face of federal de-prioritization of such rights.[226] In general, the article suggests that consumer protection and employment rights are areas that are "ripe" for qui tam enforcement.[227] To overcome issues of Article III standing, class certification, and arbitration in traditional rights-enforcement schemes, Gilles and Friedman argue that an agency relator model for these qui tam provisions is preferable, and that drafters should be clear that the "relator represents the *state*, in its law enforcement capacity, and no one else."[228]

Another highly relevant proposal argues for the application of qui tam enforcement mechanisms in statutes that frame privacy as a public right.[229] In his 2022 proposal, Professor Peter Ormerod takes issue with the structure of the United States

---

223. *See generally, e.g.*, Gilles & Friedman, *supra* note 27 (advocating for a "new" qui tam); Ormerod, *supra* note 28 (advocating for qui tam in privacy laws).

224. *See generally* Gilles & Friedman, *supra* note 27 (calling for the implementation of new qui tam laws).

225. *See id.* at 490 (describing the current sentiment towards rights enforcement).

226. *See id.* at 491 ("[A]s federal enforcers signal disinterest in the rights of vulnerable communities, and as the federal judiciary forecloses private avenues for enforcing those rights[,] we are left with an enforcement gap. . . . Qui tam allows the state to conserve resources by tapping the powerful force of the citizenry . . . .").

227. *See id.* at 491, 516 (discussing potential qui tam integration in new areas).

228. *See id.* at 523 (discussing potential solutions to preemption issues).

229. *See generally* Ormerod, *supra* note 28 (discussing qui tam implementation from a privacy point of view).

privacy law framework, finding not only that it has serious enforceability issues, but also that it promotes mere administrative, checkbox-ticking compliance over substantive standards for data protection.[230] He then argues that qui tam mechanisms are a solution to the woes of traditional privacy law enforcement because qui tam allows for more rigorous enforcement than current regulatory schemes while also sidestepping the issues that plague private enforcement.[231] Ormerod acknowledges that, as qui tam is only available for the vindication of public rights,[232] its use in the enforcement of privacy rights would require a reframing of privacy from an individual right, or a right to "solitude" in the face of technological advancements that oppose it,[233] to a collective right, a right focused on interpersonal "boundary management."[234]

Importantly, both articles explain that, in qui tam statutes, the relator may either act as an "agent" of the Government, merely inhabiting the Government's place in prosecuting the claim, or as an "assignee" of the Government's claim.[235] For actions brought under the FCA, the relator primarily operates under the assignment model, and the Government seemingly must suffer an injury-in-fact for standing because the FCA "gives the relator himself an interest *in the lawsuit*, and not merely the

230. *See* Ormerod, *supra* note 28 at 279 (discussing issues that arise with qui tam in the privacy framework); *see also supra* Part I.C (discussing the procedural and substantive challenges of traditional enforcement of security laws).

231. *See* Ormerod, *supra* note 28, at 315 (discussing findings on qui tam's potential implementations).

232. *See* Ormerod, *supra* note 28, at 316–19. This goes to the very nature of qui tam—relators sue on behalf of the Government for the remedy of a governmental or "public" harm. *See supra* Part II.A (describing qui tam's traditional usage).

233. *See* Ormerod, *supra* note 28, at 316 (describing the right to privacy as an individual's "right to be let alone" (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 193, 196 (1890))).

234. Ormerod, *supra* note 28, at 317 (citing Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906 (2013)); *see also id.* at 316–18 (explaining how privacy may be considered a social phenomenon rather than an individual right).

235. *See* Gilles & Friedman, *supra* note 27, at 521–22 (discussing the agency and assignment models); *see also* Ormerod, *supra* note 28, at 320–22 (discussing the same).

right to retain a fee out of the recovery."[236] The "new" state-level qui tam, Gilles and Friedman argue, should instead adopt the agency model, where the relator relieves themselves of all control over the case once the Government steps in.[237] Ormerod similarly argues that, in order to be effective in the face of judicial challenges, a qui tam privacy statute should model its procedure and damages on the FCA, but adopt an agency relator model.[238] This is because the agency model merely enforces the Government's prosecutorial powers, thus eliminating any injury-in-fact requirement, as the governmental injury "to its sovereignty arising from the violation of [the statute]" is sufficient for the Government to pursue on its own.[239]

In sum, qui tam enforcement mechanisms are unique and effective statutory provisions that give private individual relators the power to sue on behalf of the government. Notably, the FCA, operating primarily under its assignment model, has been the most effective example of qui tam in recent U.S. law, and has even found some success in data security enforcement through the DOJ's CCFI. Newer qui tam proposals, including collective rights and privacy rights enforcement proposals, suggest that applying agency-relator-model qui tam provisions to statutes can better effectuate enforcement regimes by sidestepping common issues within the regimes. Part III builds on this framework to argue that federal data security legislation should include a qui tam mechanism to better accomplish data breach prevention and deterrence.

III. SECURITY QUI TAM: AN INTEGRATIVE SOLUTION

So far, this Note has provided an overview of data security law in the United States and highlighted key enforcement issues

236. Gilles & Friedman, *supra* note 27, at 522 n.164 (quoting Vermont Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 772 (2000)); *see also supra* Part II.A.1 (explaining that, if the Government chooses not to intervene, the relator may nonetheless proceed with the action on its own).

237. *See* Gilles & Friedman, *supra* note 27, at 522 (describing how a "new" qui tam would fit into the agency mold).

238. *See* Ormerod, *supra* note 28, at 320–22 (explaining that choosing an agency relator model aligns with the Supreme Court's dicta in *Stevens*).

239. *See Stevens*, 529 U.S. at 774; *see also* Gilles & Friedman, *supra* note 27, at 522–23 (describing the workings of an agency model).

with current and developing enforcement regimes.[240] Specifically, this Note has explained that public enforcement is often too difficult for agencies to pursue, and private enforcement often fails for procedural reasons.[241] Further, both suffer from a major flaw in the context of data breaches: enforcement occurs too late.[242] Part II of this Note gave an overview of qui tam enforcement mechanisms, especially in the context of the FCA, suggesting that they may be of use in the data security regime.[243] Recent proposals for new statutes that utilize qui tam provisions to enforce consumer protection rights, employment rights, and privacy rights further demonstrate the potential for qui tam to operationalize underenforced sectors of the law.[244] This Part argues that Congress should add qui tam provisions in data security legislation to mend the enforcement gap that plagues the data breach legal landscape. It does so by setting forth two plausible applications—one using the agency relator model and another using the assignment relator model. While this Note posits that an agency relator model is likely preferable as it allows complete enforcement before any breach need occur, both models have their comparative strengths, and this Part concludes with a discussion of those strengths.

A. QUI TAM PROVISIONS CAN PROVIDE AN UPGRADE TO DATA SECURITY ENFORCEMENT

With an understanding that public agency enforcement and private rights of action have proven insufficient to adequately address data security concerns, Congress should look to qui tam provisions to fill the enforcement gap. The FCA allows private individuals with knowledge of fraud against the government to protect the public's interest in ensuring taxpayer dollars are

240. *See supra* Part I.B–I.C (discussing the context of data privacy law and its enforcement issues).

241. *See supra* Part I.C (explaining the issues involved with public and private enforcement).

242. *See supra* Part I.C.1 (discussing the timing issue of enforcement).

243. *See supra* Part II.A.3 (discussing the successful application of the FCA in the DOJ's Civil Cyber-Fraud Initiative, which bolstered data security enforcement in relation to entities sufficiently tied to government operations).

244. *See supra* Part II.B (explaining the "new qui tam" proposal by Gilles & Friedman as well as the "privacy qui tam" proposal by Ormerod).

properly accounted for.[245] Likewise, a security qui tam law would allow private individuals with knowledge of insufficient security protocol to protect the public's interest in secure data.[246] Importantly, a security qui tam law would allow relators to enforce data security standards before a breach need occur.[247] While Congress could feasibly amend any one of the many sectoral security laws to include a qui tam provision to bolster enforcement,[248] this Part focuses on two potential types of general applications: the first being a certification scheme under the agency relator model and the second being a government harm scheme under the assignment relator model.

1. A Governmental Interest in the Economy of Data: The ADPPA Certification Scheme

One plausible application of a qui tam provision to a data security law would be in a certification scheme, whereby data-controlling entities regularly certify to the government that they are following sufficient security standards.[249] For example, a qui tam mechanism in a reintroduced version of the ADPPA could very well provide for effective relator enforcement of compliance

---

245. *See supra* Part II.A (discussing how public interests are protected under the FCA).

246. This public interest comprises various costs arising from breaches, including individual costs, corporate (data-handling entity) costs, economic costs, and government administration costs, to name a few. *See* Riedy & Hanus, *supra* note 35, at 16–21 (discussing the aggregate consumer costs and high costs to entities when breaches occur); *see also supra* note 22 and accompanying text (discussing the many various harms of data breaches).

247. *See supra* Part III.A (describing the ability of a relator to bring a case and the government to intervene, both before a breach has occurred).

248. *See supra* notes 62–67 and accompanying text (discussing the myriad of federal privacy and security statutes).

249. Note that the FCA also has a certification provision. *See* 31 U.S.C. § 3729(a)(1)(A) ("[A]ny person who . . . knowingly presents, or causes to be presented, a false or fraudulent claim for . . . approval . . . is liable to the United States Government . . . ."). However, for an FCA false certification claim to be successful, the false certification must cause "the government to pay out money or forfeit moneys due." United States *ex rel.* Markus v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240, 1241 (E.D. Cal. 2019). This is because the FCA operates under an assignment relator model, requiring an injury-in-fact on behalf of the Government to succeed. *See*, *e.g.*, Ormerod, *supra* note 28, at 319–21 (discussing the FCA's assignment model). Like in Ormerod's proposal, the certification scheme should also provide that the relator's share is no more than a fee received from the Government's recovery to reinforce the agency relator model. *See id.* at 322.

within a security certification scheme.[250] The original ADPPA proposed, among other privacy and security provisions, that entities be required "to adopt data security practices and procedures that are reasonable in light of the entity's size and activities."[251] In addition, the ADPPA would have required that an executive officer of an entity "certify, in good faith," to the government that its data security practices are in compliance with the act.[252] Despite having bipartisan support in both houses of Congress, the proposed act stalled, in part due to debate over its enforcement.[253] Qui tam can settle this debate by offering a mechanism that allows for broader enforcement than public enforcement alone, thus prompting compliance with the statute, while simultaneously quelling concerns of disparate district court outcomes resulting from private litigation by placing the suits in the hands of the Government.[254]

While the ADPPA's proposed certification scheme serves as an adequate basis for a qui tam security statute, the new statute should explicitly delineate specific standards to which data-controlling entities must certify compliance, rather than rely on a "reasonableness" standard.[255] Such a change is necessary not

250. *See supra* note 26 and accompanying text (discussing the American Data Privacy and Protection Act, proposed in 2022, that stalled in Congress). Note that the subsequently proposed American Privacy Rights Act (APRA) contains largely the same substantive obligations on data handling entities, although there are slight variations regarding the scope, timing, and preemptive impact of certain provisions. LINEBAUGH ET AL., *supra* note 137, at 5–6. For the purposes of this proposal, these changes are minimal.

251. GAFFNEY ET AL., *supra* note 26, at 2; *see also* H.R. REP. NO. 117-669, at 22 (2022) (requiring covered entities to "establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures").

252. H.R. REP. NO. 117-669, at 24 (2022).

253. *See* GAFFNEY ET AL., *supra* note 26, at 1, 4–5 (discussing congressional support for the ADPPA, reasons for its failure, and fears by some state attorneys general that the ADPPA would "set a 'ceiling' for privacy rights rather than a 'floor'").

254. *See* Qiuyang Zhao, *American Data Privacy and Protection Act: Latest, Closest, Yet Still Fragile Attempt Toward Comprehensive Federal Privacy Legislation*, JOLT DIGEST (Oct. 19, 2022), https://jolt.law.harvard.edu/digest/american-data-privacy-and-protection-act-latest-closest-yet-still-fragile-attempt-toward-comprehensive-federal-privacy-legislation [https://perma.cc/A728-53VY] (noting the backlash from businesses over a private right of action because it may create further confusion over disparate district court outcomes).

255. *Cf.* H.R. REP. NO. 117-669, at 24 (2022) (outlining corporate accountability and certification requirements under the ADPPA).

because of any substantive issue with the duty of "reasonableness," but because the context of the potential enforcement lawsuit is shifted from being post-breach to pre-breach.[256] Delineating specific standards is thus necessary in order to limit the volume of potential claims to only the most viable and provide potential relators with clear standards for bringing a potential suit. The qui tam security statute may look to the DOJ's CCFI cybersecurity enforcement under the FCA for guidance in this endeavor, requiring, for example, compliance with National Institute of Standards and Technology (NIST) standards specific to the entity's relevant industry and business size.[257]

Further, a certification-based security qui tam statute should explicitly adopt an agency relator model and disclaim the assignment model to ensure that injury-in-fact requirements are not of issue.[258] Because the agency model is "predicated on the [G]overnment's general enforcement powers," private individuals assert and prosecute claims for the Government "as its subordinate agent" without a need for relators to incur injuries-in-fact to themselves, nor for the Government to suffer an injury-in-fact to itself.[259] Rather, the claim may proceed on the premise

256. *See supra* Part I.C.1; *infra* Part III.B.1.

257. *See, e.g.*, *supra* Part II.A.3 (discussing the Civil Cyber-Fraud Initiative and its certification requirements with NIST standards for entities that contract with the government); *see also NIST Cybersecurity Framework*, NIST: SMALL BUS. CYBERSECURITY CORNER (May 1, 2024), https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0 [https://perma.cc/64NN-RSBH] (providing a framework of "standards, guidelines, and practices to help organizations to better manage and reduce cybersecurity risk"). Such standards may cover encryption requirements, authentication requirements for employee or consumer access, or data deletion requirements, for example. *See Securing Data & Devices*, NIST: SMALL BUS. CYBERSECURITY CORNER (Aug. 23, 2024), https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/securing-data-devices-1 [https://perma.cc/SC5V-UD7P].

258. *See* Ormerod, *supra* note 28, at 320 ("The statute should . . . explicitly adopt the agency model and should disclaim the assignment model . . . . [T]he relator is 'simply the statutorily designated agent of the [government], in whose name . . . the suit is brought—and that the relator's bounty is simply the fee he receives out of the [government's] recovery for filing and/or prosecuting a successful action on behalf of the Government.'" (quoting Vermont Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 772 (2000))); *see also supra* Part II.B (discussing the agency and assignment models of relators in qui tam statutes discussed in the Gilles & Friedman proposal); Gilles & Friedman, *supra* note 27, at 521–22 (describing the ability of the agency relator model to circumvent injury-in-fact requirements).

259. Gilles & Friedman, *supra* note 27, at 521–22.

of injury to the Government's "sovereignty arising from violation of its laws," which the Supreme Court has confirmed to be sufficient in sustaining government criminal lawsuits.[260] To further protect against constitutional challenges, it may also be necessary to include a clause that explicitly terminates the relator's prosecutorial power over the action once the qui tam action is filed.[261]

This type of security qui tam statute would allow private individuals, such as employees of data-controlling entities, to bring suits on behalf of the Government when the entities falsely certify that they are meeting prescribed data security standards.[262] Such a statute addresses the rampant underenforcement of security laws and allows for the addressing of substandard data practices before the costs of a breach impact individuals, the entity, and society as a whole.[263] Further, as courts have discussed in the context of FCA lawsuits, Article III standing is not an issue because the relator is acting only for the Government to vindicate public interests, rather than their own interests.[264]

In adopting an agency relator model, the certification scheme has a few limitations. For one, if the Government intervenes, the relator has no right to continue as a participant in the litigation.[265] In addition, the relator has no right to contest if the Government later decides to voluntarily dismiss the suit, nor do they have the right to demand a judicial determination regarding any settlement.[266] While these limitations are necessary to

260. *Stevens*, 529 U.S. at 772; *see also* United States *ex rel.* Polansky v. Exec. Health Res., Inc., 143 S. Ct. 1720, 1727 (2023) (confirming the sufficiency of this premise of injury). The agency theory is further supported by numerous historical qui tam laws. *See Stevens*, 529 U.S. at 777.

261. *See supra* note 183 (discussing a recent district court's holding that the FCA's qui tam provision violates the Appointments Clause).

262. *See supra* notes 237–39 and accompanying text (describing the arguments in favor of the agency relator model).

263. *See supra* Part I.C (explaining that security standards are underenforced under the current data security laws); *supra* Part I.C.1 (describing the timing issue of current data security laws).

264. *See supra* Part II.A.2 (discussing the FCA's resilience in the face of constitutional challenges).

265. *See* Ormerod, *supra* note 28, at 320 (describing a limitation from the FCA that would also be present in the proposed agency model).

266. *See id.* (comparing further the proposed agency model with the FCA's qui tam provision). The certification scheme should also specify that a qui tam claim under the statute cannot be joined with a private claim to separate the

best ensure that the qui tam provision survives any constitutional objections, they mean that, once brought, the Government has the lion's share of discretion in prosecuting the case.[267] Nevertheless, the agency-relator-based certification scheme would bridge the vast oversight and enforcement gaps of the current data security enforcement regime,[268] even if the Government chooses to dismiss any number of cases. In sum, a qui tam compliance certification scheme, while having limits, has the potential to significantly address the shortcomings of traditional data security enforcement.

2. A Governmental Interest in Its Own Identifiers: Taking Control of Social Security Numbers

Another plausible means for qui tam security enforcement is to tie the qui tam provision to a statute establishing a standard of care for securing a specific type of data which the government has significant interest in protecting, such as SSNs. This type of government interest scheme is far narrower than a certification scheme; it is limited in scope to entities that collect a specific type of sensitive data and potentially requires some governmental injury beyond statutory damages.[269] However, it can be modeled more closely after the well-settled FCA qui tam application,[270] and nonetheless may reach a majority of entities that handle sensitive consumer data.

By tying the qui tam provision to security enforcement of a type of data in which the government has a particular interest, legislatures may employ the assignment model—the same relator model used in the FCA[271]—in structuring the qui tam enforcement mechanism. Like in the FCA, doing so allows the relator to remain a party, even when the Government intervenes

---

relator from representing their own interests. Gilles & Friedman, *supra* note 27, at 536 (stating that the FCA behaves similarly to "avoid[] revenue-depressing conflicts of interest").

267. *See* Ormerod, *supra* note 28, at 320 ("Scrupulously adhering to an agency model therefore necessitates embracing the government's ultimate authority to control the action and its resolution.").

268. *See supra* Part I.C.

269. *See* Gilles & Friedman, *supra* note 27, at 522 (describing the injury requirements of the agency model under the FCA).

270. *See supra* Part II.A (describing the FCA and its qui tam provision).

271. *See* Vermont Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 773 (2000) (describing how the FCA assignment relator model operates).

in the case, because the Government partially assigns "its claim to redress its injury to the relator, who acquires standing on that basis just like any assignee."[272] This also means that a relator may choose to continue the suit, even if the Government chooses not to intervene for any reason.[273] Importantly, this scheme, like the FCA, would also allow the Government to intervene later on to dismiss the case in order to regulate the enforcement of the scheme.[274]

In this government interest scheme for security qui tam, the governmental harm could be, for example, the administrative and actual costs resulting from the inadequate protection of the data at interest. The government interest scheme for security qui tam may also model its procedural structure after the FCA, in addition to its monetary civil penalty and damages.[275]

One limitation of this scheme is that, while courts *might* hold that statutory damages owed to the Government satisfy relator Article III standing,[276] it is more likely that a court would require that the Government suffer at least *some* injury-in-fact to confer standing.[277] It follows that qui tam relators under the government interest scheme may only be able to sue post-breach. Nonetheless, relators under this scheme may still bring suits more quickly and based in more personal knowledge of the entity-in-question's security standards than breach victims or government enforcers.[278] Further, qui tam's ability to sidestep other issues of traditional enforcement—such as class certification woes, breach victims' standing, and forced arbitration—potentially increases the likelihood of successful litigation, serving as

---

272. Gilles & Friedman, *supra* note 27, at 522 (citing *Stevens*, 529 U.S. at 773).

273. *Id.* Note, however, that the Government may choose to intervene and dismiss the case at any later point. United States *ex. rel.* Polansky v. Exec. Health Res., Inc., 143 S. Ct. 1720, 1736 (2023).

274. *See supra* note 163 and accompanying text (describing the power of the Government to intervene and dismiss cases under the FCA).

275. *See supra* Part III.A.

276. *See Stevens*, 529 U.S. at 773 ("The FCA can reasonably be regarded as effecting a partial assignment of the Government's damages claim.").

277. *See id.* at 774 ("[T]he United States' injury in fact suffices to confer standing on [the relator].").

278. *See supra* Parts II.A–II.B (discussing the benefits of qui tam, including harnessing the relators' personal knowledge of alleged wrongdoing).

a larger deterrent to data-controlling entities that operate using substandard security measures.[279]

One example of how this scheme could work is in a statute explicitly requiring that any entity that collects, stores, or otherwise uses consumers' SSNs adopt reasonable security standards to safeguard the data. Including a qui tam provision in such a statute would allow relators, presumably employees of an entity or other individuals who have explicit, non-public knowledge of an entity's substandard security practices,[280] to bring forth a suit to enforce the protection of SSNs. While more limited than the certification scheme, this type of security qui tam could still be fairly far-reaching in its enforcement capabilities. For example, over sixty-four percent of data breaches reported in 2022 included the compromise of full SSNs.[281] In addition, use of exposed SSNs can lead to billions of dollars in potential governmental damages.[282] To best effectuate this qui tam enforcement provision, the statute should include a comprehensive "Purposes & Findings" section explicitly stating the harms the government suffers from exposed SSNs to guide potential relators as to when an action may be brought.[283] For example, the section may dictate a purpose of "encourag[ing] private parties to recover civil penalties for the government that otherwise may not have been

279. *See supra* Parts I.C–I.D (discussing the issues with traditional enforcement following data breaches).

280. *See, e.g.*, Bryan Lemons, *An Overview of "Qui Tam" Actions*, FED. L. ENF'T TRAINING CTRS. (Mar. 30, 2024), https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/civil-actions/quitam.pdf [https://perma.cc/4QNU-AUPN] ("While virtually anyone can be a relator, the majority of those who bring 'qui tam' actions are current or former employees, who have an insider's perspective on the wrongdoing.").

281. *See 2022 Data Breach Report*, IDENTITY THEFT RES. CTR. (Jan. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf [https://perma.cc/5P87-NHXL] (reporting that 1,143 of the 1,774 data breaches in 2022 included full Social Security Numbers).

282. *See* Press Release, Internal Revenue Serv., IRS Criminal Investigation Releases Annual Report Highlighting 2,500+ Investigations, Law Enforcement Partnerships (Nov. 18, 2021), https://www.irs.gov/newsroom/irs-criminal-investigation-releases-annual-report-highlighting-2500-plus-investigations-law-enforcement-partnerships [https://perma.cc/489Y-8LAP] (noting that the Internal Revenue Service uncovered $10 billion in tax fraud schemes in 2021 alone).

283. *See* Ormerod, *supra* note 28, at 318–19 (discussing the merits of an explicit findings and purposes section in "fortifying the proposal against arguments that it constitutes an exotic and unprecedented use of qui tam").

successfully assessed by overburdened . . . enforcement agencies."[284]

In sum, security qui tam can address many of the issues identified in the current enforcement scheme while adding new promises in data security law.[285] Whether through a certification scheme, a government interest scheme, or both, Congress should look to bolster the defenses against data breaches through enactment of a qui tam security statute. The next Section further explores the benefits of qui tam in the context of a federal data security statute.

B. EMBRACING THE PROMISES OF SECURITY QUI TAM

This Note's security qui tam proposal builds on other scholars' recent and burgeoning recognition of qui tam as a powerful, important, and overlooked tool in American jurisprudence.[286] However, this proposal diverges from others in a few ways.[287] First, this proposal backs scholarly enthusiasm with proof-of-concept, by way of the DOJ's Civil Cyber-Fraud Initiative encouraging use of qui tam to improve data security standards for a small subset of all data-handling entities.[288] Further, this proposal is narrowly tailored to a discrete issue in security law.[289] It does not purport to revolutionize or upend an entire practice or industry. Nonetheless, it may better effectuate the deterrence and prevention of breaches through the institution of an enforcement mechanism that has already withstood numerous legal challenges. The development of security law is notoriously

---

284. *Id.* at 318 (quoting Gilles & Friedman, *supra* note 27, at 512).

285. *See supra* Part I.C (discussing the shortcomings of traditional enforcement).

286. Specifically, this Note builds upon the analyses of Ormerod, Gilles & Friedman, and Engstrom. *See generally* Ormerod, *supra* note 28; Gilles & Friedman, *supra* note 27; Engstrom, *supra* note 176.

287. Critically, this Note proposes qui tam to address breaches as a subdivision of privacy and security law because the author of this Note has concerns about the feasibility of reframing privacy as a societal right as opposed to an individual right.

288. *See supra* Part II.A.3 (discussing recent settlements under the Civil Cyber-Fraud Initiative).

289. *Cf.* Ormerod, *supra* note 28, at 327 (discussing "operationalizing" privacy theory by reframing privacy as a public right rather than an individual right).

sticky, as major changes in federal policy are rare.[290] This proposal aims to add to the scholarly discussion by proposing an incremental, enforcement-based improvement to a subset of security law, rather than upending the entire theory behind the law. This Section elaborates on qui tam's effectiveness in sidestepping traditional barriers to security enforcement, its administrative resiliency, and its ability to better deter breaches.

1. Correcting Incentives and Deterrence: Enforcement Before the Breach

Security qui tam significantly addresses substantive enforcement concerns. Most importantly, security qui tam allows enforcement of substandard data security practices without the necessity of a large-scale breach by empowering relators to bring an earlier suit based on their own knowledge, supported by evidence, of the substandard practices *before* a breach occurs.[291]

Further, as an integrative, win–win solution, qui tam spares individuals the emotional and actual costs of their data being exposed, and, by avoiding a breach altogether, spares data-controlling entities the massive expenses of post-breach damage control.[292] Security qui tam thus realigns the incentives for data-controlling entities by increasing the likelihood that enforcement is actually and successfully brought.[293] As a result, data-controlling entities would be more likely to ensure that they meet the standards imposed under the qui tam statute.

In addition, data-controlling entities have called for a federal general data privacy and security statute in recent years to standardize and clarify the duty of care that they owe regarding consumer data.[294] Entities express that such a statute would

290. *See supra* Part I.B (discussing the history of privacy and security law in the United States, specifically noting that the operational theory behind many laws has largely remained the same since the advent of the telegraph).

291. *See supra* Part III.A (discussing how the proposal enables relators to bring an action before a breach occurs).

292. *See supra* Part I.C (discussing the massive costs to data-controlling entities of breaches).

293. *See supra* Part I.C.2 (explaining that the improbability of a successful litigation action or agency enforcement provide poor incentives for data-controlling entities to properly ensure reasonable security standards).

294. *See* Zhao, *supra* note 254 ("[P]reemption is welcomed by businesses as it would stop the patchwork of state privacy laws and make the privacy regulatory framework across the US easier to comply with.").

actually *save* them in compliance costs by enforcing a uniform standard across jurisdictions and industries.[295] The security qui tam proposal thus has the potential to lower compliance costs for entities by facilitating agreement on the enforcement of a federal statutory proposal.[296]

While critics may posit that qui tam enforcement mechanisms could lead to "an explosion" of frivolous litigation and increased compliance and litigation management costs for data-controlling entities,[297] these concerns are misplaced. With qui tam, the government can serve as a floodgate to the litigation concerns, choosing not to intervene in, or even choosing to dismiss, suits brought under qui tam that it views as insufficiently pled or not worth pursuing.[298] This is supported by recent empirical scholarship, finding little support for the "increased litigation" concerns surrounding the FCA and qui tam;[299] instead, scholars have described a "steady maturation" of qui tam enforcement since the 1986 amendments, with continuing efficacy and efficiency even as settlements grow in size.[300]

2. Sidestepping the Issues of Traditional Enforcement

Additionally, security qui tam sidesteps the procedural issues that burden private litigation including adhesion contracts, Article III standing, and class certification.[301] Adhesion contracts that force arbitration or otherwise result in individuals waiving their ability to sue do not apply to qui tam claims because the claims belong to the Government.[302]

---

295. *Id*.

296. *See supra* Part III.A.1 (discussing the benefits of security qui tam in a federal data protection proposal such as the ADPPA).

297. *See* Cohen, *supra* note 166, at 96 (expressing concern of expanding litigation under the 2009 FCA amendments).

298. This is even clearer if security qui tam models its pleading standards after the FCA, using the heightened standard required in cases of pleading fraud and requiring cases to be filed alongside evidence of the alleged violation. *See* FED. R. CIV. P. 9(b); 31 U.S.C. § 3730(b)(2).

299. *See* Ormerod, *supra* note 28, at 311–12 (citing Engstrom, *supra* note 176, at 1951–63).

300. Engstrom, *supra* note 176, at 1996–97.

301. *See supra* Part I.C.

302. This result has been confirmed in the context of the FCA, especially when there is no relator injury requirement. *See* Ormerod, *supra* note 28, at 325–26 (citing multiple FCA cases where courts have confirmed the viability of FCA claims despite arbitration clauses).

Article III standing poses a lesser barrier to qui tam actions because, in the case of the agency relator model, the suit is solely that of the Government exercising its enforcement powers, while in the assignment relator model, the injury-in-fact requirement is satisfied by a financial injury to the Government.[303] Security qui tam also avoids class certification issues by avoiding classes entirely—the suit belongs to the Government, with the relator being awarded a fee for their relating "services."[304] Finally, by awarding successful relators with a portion of the Government's damages award,[305] rewards are more ascertainable pre-suit and thus would-be plaintiffs are more inclined to pursue an action than when seeking remedies on their own.[306]

In sum, security qui tam enables the remedy of substandard security practices before a breach occurs, allowing for clearer incentives for entities to meet their standards for data security. Additionally, security qui tam shifts the timing of litigation expenses on data-controlling entities to before a breach, when they are more manageable, rather than adding to other costs post-breach. By enabling enforcement for security standards earlier and more often than in the current regime, security qui tam can more effectively deter and prevent breaches and, as a result, lower the harms that result from breaches. In other words, security qui tam can give teeth to the current data security enforcement regime.

CONCLUSION

The data economy is huge—and growing—and offers enormous potential for enrichment of the human experience. With that potential, however, comes the risk of harms associated with the improper use or exposure of individuals' personal and sensitive data. Despite the breach epidemic raging since 2005,

303. *See supra* Parts II.A.1–A.2 (discussing Article III and the FCA); *see also* Ormerod, *supra* note 28, at 326 (stating that injury-in-fact requirements apply only to private rights of action).

304. *See supra* Part II.A.1 (explaining how qui tam suits belong to the Government).

305. *See supra* Parts II.A.1–A.2.

306. *See supra* Part I.C (discussing the high risk and low reward of bringing a lawsuit as a breach victim due to the difficulties in ascertaining and the low individual value of post-breach anxiety). Furthermore, the bulk of the costs of the litigation are on the Government, rather than individual Plaintiffs. *See supra* Part I.C.

lawmakers have been markedly uncreative and unreactive in addressing it. While breaches cost entities billions and raise the collective anxiety of the United States, federal privacy and security law remains mired in ineffective concepts and frameworks.

Recently, however, scholars and experts have sought to advance the framework for privacy and security by offering creative solutions to this tired regime. This Note seeks to contribute to that effort by proposing more effective data security enforcement without compromising the value and potential of data. By enabling better enforcement, security qui tam can substantiate the duty of data-controlling entities, realign incentives for protecting sensitive data, and reduce the prevalence and impact of data breaches.