BYU Law Review

Volume 49 | Issue 2 Article 11

Winter 12-27-2023

Byte a Carrot for Change: Uprooting Problems in Data Privacy Regulations

Sarah Terry

Byte a Carrot for Change: Uprooting Problems in Data Privacy Regulations

Sarah Terry[*]

There is a growing gap between technology advancement and a lagging regulatory system. This is particularly problematic in consumer data privacy regulating. Companies hold collected consumer data and determine its use largely without accountability. As a result, ethical questions that carry society-shaping impact are answered in-house, under the influence of groupthink, and are withheld from anyone else weighing in.

This Note poses a solution that would address multiple data privacy regulation issues. Namely, an incentive approach would help even out the information-imbalanced system. Incentives are used as tools throughout intellectual property law to foster commercial progress, discourage trade secrets, and protect consumers. These goals can also be achieved through integrating an incentive into consumer data privacy regulating.

This Note first highlights major issues in the current consumer data privacy federal regulatory landscape. Next, this Note proposes and outlines a narrow FTC whistleblower incentive, unearthing how an incentive would alleviate each major regulatory issue. Finally, this Note discusses eight compelling reasons for the incentive, and ultimately confronts and rebuts its drawbacks.

* J.D., BYU Law School, 2023. I thank Professor Clark Asay for his thoughtful insight and guidance on this Note during the drafting process. I also thank the fabulous BYU Law Review team of editors who contributed their time and many talents. Finally, I thank my family for supporting me in so many meaningful ways throughout this endeavor.

CONTENTS

INTRODUCTION

Shortly after the launch of ChatGPT, the most disruptive technological innovation in decades, OpenAI Chief Technology Officer (CTO) Mira Murati and OpenAI co-founder Elon Musk each publicly called for regulators to get involved.[1] These calls are rooted in a notion both have openly articulated: the consumer data collected and used by ChatGPT will shape society—for better, for worse, and for now—in largely unknown ways.[2] Unknown, that is, by the public and by regulators. Companies, on the other hand, may already have a clear picture of the impacts their consumer data strategies cause. However, companies are without obligation to disclose their discoveries—including known harms—and instead hold research and findings as proprietary trade secrets.[3] As a result, ethical questions about data usage are answered in-house, under the influence of groupthink, in the interest of commercialism, and are withheld from anyone else weighing in.[4]

The United States has largely taken a consent-based approach to data privacy, letting clicked boxes or continued use[5] perform "moral magic."[6] Such consent is called into question and seriously undermined when even the experts on artificial intelligence are not

1. *See* Steve Mollman, *ChatGPT Must Be Regulated and A.I. 'Can Be Used by Bad Actors,' Warns OpenAI's CTO*, FORTUNE (Feb. 5, 2023, 1:45 PM), https://fortune.com/2023/02/05/artificial-intelligence-must-be-regulated-chatgpt-openai-cto-mira-murati; Jyoti Narayan, Krystal Hu, Martin Coulter & Supantha Mukherjee, *Elon Musk and Others Urge AI Pause, Citing 'Risks to Society'*, REUTERS (Apr. 5, 2023, 6:22 AM), https://www.reuters.com/technology/musk-experts-urge-pause-training-ai-systems-that-can-outperform-gpt-4-2023-03-29. *But see* David Shepardson, *Tesla Recalls 362,000 U.S. Vehicles over Full Self-Driving Software*, REUTERS (Feb. 16, 2023, 5:34 PM), https://www.reuters.com/business/autos-transportation/tesla-recalls-362000-us-vehicles-over-full-self-driving-software-2023-02-16 (discussing one instance Musk resisted regulators and disagreed with oversight findings for the AI-based autopilot feature in Tesla cars).

2. *See* Narayan et al., *supra* note 1.

3. *See* Lital Helman, *Trade Secrets and Personal Secrets*, 55 U. RICH. L. REV. 447, 447–63 (2021) (discussing the differences and overlap between the approaches to trade secret law and data privacy law, namely, where personal data can "belong" to both a company's trade secrets and an individual).

4. *See* Mollman, *supra* note 1.

5. *See* Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. (forthcoming 2024) (manuscript at 4), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743 [hereinafter Solove, *Murky Consent*] (discussing the fictions of consent and an argument for a revised "murky consent" approach).

6. *See* Heidi M. Hurd, *The Moral Magic of Consent*, 2 LEGAL THEORY 121, 121–46 (1996).

fully sure how consumer data is used.[7] Put simply, consumers might be aware their data is collected, but are largely unaware of the extent to which it is used and how such use is affecting them.

In 2021, a Facebook insider leaked papers demonstrating consumer data has already been used to target propagandistic untruths toward the most susceptible individuals—those most eager to believe and promulgate the sensational material.[8] A recent controversy involving Twitter in summer of 2022 revealed national security issues are at stake because an insider demonstrated that Twitter has more data than it realizes or knows what to do with.[9] But these companies did not come forward with this information willingly. These businesses decided transparency was outside their best interest. Instead, a small number of employees brought these issues to the attention of the public, risking their careers, reputations, financial security, and personal relationships, and facing legal liability against deep-pocketed tech giants.

Something needs to change. But after more than a decade of effort, federal lawmakers have yet to pass bipartisan bills that cohesively regulate consumer data privacy.[10] The American consuming public has called for it, and now even data lobbyists are on board.[11] Congress has struggled to craft these laws in part because of the difficulty in striking the right balance between consumer and commercial interests. Specifically, an overarching policy seeks federal data regulations that both adequately address

7. *See* Solove, *Murky Consent*, *supra* note 5, manuscript at 2.

8. *See* Dipayan Ghosh & Ben Scott, *Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You*, TIME MAG. (Mar. 19, 2018, 12:38 PM), https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data.

9. *Transcript: Twitter Whistleblower Testimony to Senate Judiciary Committee*, TECH POL'Y PRESS (Sept. 13, 2022), https://techpolicy.press/transcript-twitter-whistleblower-testimony-to-senate-judiciary-committee [hereinafter *Transcript*].

10. *See* Press Release, Fin. Servs. Comm., Financial Services Committee Advances McHenry's Data Privacy Act (Feb. 28, 2023), https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=408620 (discussing the latest development in federal action to enact data privacy law, the Data Privacy Act of 2023); *see also* Data Privacy Act of 2023, H.R. 1165, 118th Cong. (2023).

11. *See* Alfred Ng, *Privacy Bill Triggers Lobbying Surge by Data Brokers*, POLITICO (Aug. 28, 2022, 7:02 AM), https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958 (demonstrating that data industry lobbyists have boosted their spending after introduction of the American Data Privacy and Protection Act).

harms that may result from consumer data collection, while also refraining from over-burdening commercial innovation.[12]

This Note proposes one "ingredient" to help solve the many challenges regulators face. Namely, a garden-variety, incentive-based "carrot" to help regulate and address defects in federal data privacy law. Incentives are an integral part of intellectual property law.[13] Incentives are put into place to protect creatives, inventors, and brand rights while still facilitating innovation, benefits to society, and judicial efficiency.[14] Patent law works in various ways to discourage trade secrets while still providing protection for original inventions through the use of incentives.[15] An incentive in data privacy law could facilitate a similar goal of (1) promoting commercial progress and discouraging total trade secrecy while also (2) remaining rooted in protecting consumers. Specifically, this Note argues for a narrowly drafted whistleblower incentive and protection law relating to consumer data privacy and "unfair" or "deceptive" data practices under Section 5 of the Federal Trade Commission Act (FTC Act).

This metaphorical "carrot" has eight particularly appetizing features: (1) it furthers both prongs of the above-stated policy in a balanced way; (2) it offers an efficient enforcement tool to proportionately address harms and risks of harms; (3) it serves as a counterweight balancing the highly secretive nature of data information flow in a lagging regulatory system; (4) it presents a palatable piece for the Federal Trade Commission (FTC) to build on and learn from as the FTC confront challenges in rulemaking; (5) it can be easily grafted into any current or future bundle of regulations; (6) it fosters transparency and accountability; (7) it encourages consistent investment by companies in following regulations; and (8) it offers a way to promote deterrence while providing self-sufficient funding for the FTC.

12. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 820 (2022) (discussing the goals of data privacy enforcement).

13. *See* Jeanne C. Fromer, *Expressive Incentives in Intellectual Property*, 98 VA. L. REV. 1745, 1746–89 (2012) (discussing the "broadening of incentive possibilities [in intellectual property law] from a utilitarian position").

14. *See id.*

15. *See* J. Jonas Anderson, *Secret Inventions*, 26 BERKELEY TECH. L.J. 917, 919 (2011) ("Patents are often conceptualized as a means of luring secret inventions out of the dark, shadowy cave of trade secrecy, and into the bright, public sunlight of the patent system.").

In Part I, this Note first gives an overview of the FTC—the primary avenue to currently address data privacy laws in the United States at the federal level. Part II gives a synopsis of some relevant deficiencies and inefficiencies that result from the current FTC approach. This highlights the need for the incentive and protection law because the "carrot" addresses each of the mentioned deficiencies in at least one important way.

Part III builds on one specific inadequacy discussed above to help illustrate why the incentive is a solution to a not-fully-unearthed problem. Namely, the current system inadequately addresses known harms and is unable to gain a better understanding of lesser-known harms. There is first a discussion of known harms that result from inadequate consumer data privacy laws. Next, an analogy illustrates a fundamental reason why adequately addressing harms in consumer data privacy is uniquely challenging.

Part IV outlines and explains each carrot characteristic and why each is necessary. Part V analyzes and expands on each of the eight bits of the carrot byte, and Part VI confronts each of the carrot's potential drawbacks and challenges.

I. A NARROW OVERVIEW OF THE FTC'S CURRENT DATA PRIVACY REGULATORY LANDSCAPE AND ITS PITFALLS.

For more than two decades, the FTC has been the nation's privacy agency, consistently at the forefront of the public debate on online privacy.[16] The FTC's mission statement is to protect "the public from deceptive or unfair business practices and from unfair methods of competition through law enforcement, advocacy, research, and education."[17] This mission is balanced with an additional goal: to avoid unduly burdening legitimate business activity by maintaining a "vibrant economy fueled by fair competition."[18]

16. *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022) [hereinafter Trade Regulation Rule].

17. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Oct. 9, 2023).

18. *See id.*

The FTC Act, set forth in 15 U.S.C. §§ 41–58, as amended, empowers the FTC to:

- "prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce;"[19]
- "seek monetary redress and other relief for conduct injurious to consumers;"[20]
- through rulemaking authority, "prescribe rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices;"[21]
- "gather and compile information and conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce;"[22]
- "make reports and legislative recommendations to Congress and the public[;]"[23] and
- act as "the only federal agency with both consumer protection and competition jurisdiction in broad sectors of the economy."[24]

Section 5 of the FTC Act provides the principal legal authority for the FTC to regulate privacy and data security.[25] Section 5 prohibits "deceptive" or "unfair" commercial acts or practices.[26] A representation, omission, or practice is deceptive under Section 5 if it "is likely to mislead consumers acting reasonably under the circumstances," and is material to consumers—that is, it would

19. *Federal Trade Commission Act*, FED. TRADE COMM'N, https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act (last visited Oct. 30, 2023).

20. *Id.*

21. *Id.*

22. *Id.*

23. *Id.*

24. *About the FTC*, *supra* note 17.

25. *See* 15 U.S.C. § 45; *see also A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/mission/enforcement-authority (last updated May 2021). The FTC has rulemaking and enforcement authority over several federal laws, including the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506; Telephone Consumer Protection Act (Do-Not-Call Provisions), 15 U.S.C. §§ 6151–6155; CAN-SPAM Act, 15 U.S.C. §§ 7701–7713; HITECH Act, 42 U.S.C. §§ 17937 and 17953; and Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq. However, this Note narrowly focuses on Section 5 of the FTC Act.

26. 15 U.S.C. § 45.

likely affect the consumer's conduct or decision with regard to a product or service.[27] Generally, an act or practice is unfair under Section 5 if (1) "it causes or is likely to cause substantial injury to consumers[,]" (2) consumers cannot reasonably avoid the injury themselves, and (3) benefits to consumers or competition do not outweigh the injury.[28]

Currently, the FTC approaches privacy and data security through case-by-case enforcement and general policy work.[29] FTC enforcement actions are based on allegations that certain practices violate Section 5 of the FTC Act or other federal or state statutes to the extent these actions have harmed or pose the risk of harm through physical security, cause reputational or economic injury, or involve undesirable intrusions into the daily lives of customers.[30]

The FTC has brought actions including:

- an action against Abika.com, for secretive collection and sales of detailed consumer phone records obtained through false pretenses and without required consumer consent;[31]
- an action against CafePress, for its alleged failure to put into place and apply reasonable measures to protect consumers' personal information, and subsequently covering up a resulting breach;[32]
- an action against Twitter seeking civil penalties, permanent injunction, and monetary relief for collecting consumers' phone numbers and email addresses to improve social media account security, but also deceptively using that data to allow companies to target advertising in violation of an existing settlement agreement;[33]
- an action against Google and its subsidiary YouTube for allegedly illegally collecting personal information from

27. Cliffdale Assocs., 103 F.T.C. 110, 174 (1984).

28. 15 U.S.C. § 45(n).

29. *See* Trade Regulation Rule, *supra* note 16.

30. *See id.* at 51278.

31. *See, e.g.*, Complaint for Injunctive and Other Equitable Relief, Fed. Trade Comm'n. v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009) (No. 06CV0105D).

32. *See, e.g.*, Complaint, Residual Pumpkin Entity, LLC, Nos. C-4768, C-4769, 2022 WL 2355879 (F.T.C. June 23, 2022).

33. *See, e.g.*, Complaint for Civil Penalties, Permanent Injunction, Monetary Relief, and other Equitable Relief, United States v. Twitter, Inc., No. 3:22-cv-3070, 2022 WL 1768852 (N.D. Cal. May 25, 2022).

children without their parents' consent, where the FTC and New York Attorney General settled with the companies for a $170 million settlement;[34] and

- an action against Facebook for allegedly violating a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information. This resulted in a historic penalty with a settlement that imposed $5 billion, and significant requirements to boost accountability and transparency.[35]

Overall, the FTC brings actions when companies fail to comply with representations made to consumers about their data privacy and security practices, or when companies fail to implement reasonable security measures to protect sensitive information.

Notably, there is no private right of action for unfair or deceptive trade practices at the federal level—consumers must rely on the FTC to bring action.[36] However, because many states have state-level equivalents, state attorney generals can help fill the gaps that the FTC misses.[37] Additionally, the FTC generally cannot seek civil monetary damages except when a respondent has violated a prior settlement agreement.[38] So instead, typical FTC enforcement remedies require prohibiting acts complained of, remediating problematic acts, deleting wrongfully obtained information, modifying privacy policies, establishing a comprehensive privacy program, performing biennial audits for twenty years, and record-keeping and reporting obligations.[39] The FTC can only seek monetary penalties once a company is legally committed to one of the aforementioned remedies, the company subsequently violates

34. *See, e.g.*, Complaint, Fed. Trade Comm'n. v. Google LLC, No. 1:19-cv-02642 (D.D.C. Sept. 10, 2019).

35. *See, e.g.*, Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. Jul. 24, 2019).

36. *See* Allan Bruce Currie, *A Private Right of Action Under Section Five of the Federal Trade Commission Act*, 22 HASTINGS L.J. 1268, 1268 (1971); Moore v. N.Y. Cotton Exchange, 270 U.S. 593, 603 (1926).

37. *See* Press Release, Federal Trade Commission, Commission Seeks Public Comment on Collaboration with State Attorneys General (June 7, 2023).

38. To obtain civil monetary penalties under the FTC Act, generally, the FTC must first find a respondent has violated a previously entered cease-and-desist order. Once that hurdle is cleared, the FTC must then bring a subsequent enforcement action for a violation of that order. *See* 15 U.S.C. § 45(b)–(n).

39. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 606–25 (2014).

that agreement, the FTC becomes aware, and the FTC consequently takes action—again.[40]

There is, however, an exception where the FTC can seek monetary penalties in the first instance. Namely, the FTC Act authorizes the FTC to impose civil penalties for first-time violations of "duly promulgated trade regulation rules."[41] However, the FTC has yet to put into place trade regulation rules regarding data privacy.

The FTC published an advanced notice of proposed rulemaking (ANPR) seeking public comment on potential data privacy rules in August of 2022.[42] The ANPR noted that the FTC is "beginning to consider the potential need for rules and requirements regarding commercial surveillance and lax data security practices."[43] The ANPR includes a numbered list of ninety-five questions, with additional queries within many of the numbered questions.[44] The ANPR noted this is done to "generate a . . . record about prevalent commercial surveillance practices or lax data security practices that are unfair or deceptive, as well as about efficient, effective, adaptive regulatory responses" to help improve the FTC's enforcement work, and to inform Congress or other policymakers as they work toward reform.[45]

The size of some of the settlements and extensive obligations imposed on certain companies through FTC actions regarding data privacy might be thought to indicate an effective federal system is in place. However, there are some major deficiencies and barriers the current data privacy regulatory system must overcome. This Note's proposed "carrot" would help the FTC alleviate each of the noted barriers in at least one important way. The FTC's deficiencies are discussed below.

40. *See id.*
41. Trade Regulation Rule, *supra* note 16, at 51280; *see* 15 U.S.C. § 45(m).
42. *See* Trade Regulation Rule, *supra* note 16, at 51280.
43. *Id.* at 51277.
44. *Id.*
45. *Id.*

II. FACING FTC CHALLENGES

A. Inadequate Staffing Resources Face Increasingly Sophisticated Technology

As a preliminary matter, the FTC is without adequate resources to respond to the issues imposed by data privacy underenforcement. In September 2021, the FTC released a report to Congress, which revealed its Division of Privacy and Identity Protection had around only forty to forty-five employees.[46] With such limited resources and broad tasks—all while facing a giant industry—"short-staffed" seems like a less than adequate adjective.

To illustrate the disproportionate staff to prevalence problem, one study's statistics illustrate current commercial fraud extensiveness and its devastating potential due to inadequate enforcement: identity fraud involving use of consumers' personal information amounted to twenty-four billion dollars stolen last year, ensnaring fifteen million U.S. consumers.[47]

Further, the technology enabling these results continues to grow more sophisticated in its collection and analysis of data, thus potentially becoming more threatening. This is the case for ChatGPT, where there is already evidence it is being used to generate phishing scams to help scammers with imperfect English and poor grammar.[48] There are also forums for ChatGPT collaboration among fraudsters, demonstrating that ChatGPT is only beginning to be put to nefarious use.[49]

46. *See* FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY (2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

47. *See* John Buzzard, *2022 Identity Fraud Study: The Virtual Battleground*, JAVELIN (Mar. 29, 2022), javelinstrategy.com/2022-Identity-fraud-scams-report.

48. *See OPWNI: Cybercriminals Starting to Use ChatGPT*, CHECK POINT RESEARCH (Jan. 6, 2023), https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt.

49. *Id.*

B. The FTC's Enforcement Is Inefficient Due to Difficulty in Detectability and Lagging Regulator Expertise

Even assuming adequate resources, the FTC's enforcement power is inefficient to a point of diminishing deterrence.[50] Such inefficiency creates inconsistency in compelling companies to make proper practices a priority. The inefficiency largely exists because of the process the FTC must go through before it can seek civil penalties. The first step is likely the most formidable hurdle the FTC faces: the FTC must almost miraculously become aware of largely undetectable data practices that may be unfair or misleading. This alone is a major barrier in achieving efficiency and deterrence.

Deceptive or unfair data practices are largely undetectable because of an imbalance of information between the data industry and government. "If 'information is the "lifeblood" of effective governance,' the current prospects for effectively governing tech look dim."[51] The United States government has taken a hands-off approach, valuing technological innovation with an optimism in companies' self-regulation.[52] As a result, companies use trade secrecy arguments "to insulate themselves from oversight."[53] This has led companies to hold almost all the cards as they confront and determine how to resolve critical questions that "directly affect[] human behavior, individual rights, and freedom."[54]

Even if the first hurdle is cleared and the FTC becomes aware of a potential issue and decides to investigate, the FTC's investigative process can also be inefficient in discovering problems.[55] Inefficiency aside, the FTC has also failed to detect when a company skirted direct questions about compliance with crafty answers. An example of this was articulated in congressional testimony from Peiter Zatko, Twitter's former head of security, who

50. *See* Dianne Bartz, *Senators Criticize FTC's Reported Facebook Settlement*, REUTERS (Jul. 16, 2019), https://www.reuters.com/article/us-usa-facebook-ftc/senators-criticize-ftcs-reported-facebook-settlement-idUSKCN1UB25O.

51. Hannah Bloch-Wehba, *The Promise and Perils of Tech Whistleblowing*, 118 NW. L. REV. (forthcoming 2024) (manuscript at 11) (quoting Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L. REV. 1563, 1565 (2019)).

52. *Id.*

53. *Id.* at 13–14.

54. *Id.* at 11–12.

55. *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 165 (2015) (maintaining that it was uncertain whether the FTC had the needed tools to effectively investigate allegations of "search bias").

blew a whistle on Twitter through the SEC in July 2022.[56] Twitter had already faced FTC action and, as a result, was obligated to comply with consumer data practice audits and interviews.[57] Zatko testified that the FTC's evaluations and examinations were essentially interview questions—accepting the companies' answers as truth—and were without quantifiable measurements.[58] Zatko's disclosures led to an FTC lawsuit, resulting in Twitter being ordered to pay $150 million in civil penalties.[59]

The FTC's interview practices, combined with the example above, suggest the FTC is also lacking in the technical expertise or resources to really understand the technology it regulates and certain problems that could or actually do result. Just five years ago, an exchange on the Senate floor demonstrated the leaps and bounds required to get the lagging technical expertise of regulators up to speed:

"[ORRIN] HATCH [Senator]: . . . [H]ow do you sustain a business model in which users do not pay for your service?

[MARK] ZUCKERBERG [CEO of Facebook]: Senator, we run ads.

HATCH: I see. That's great."[60]

Since this exchange, much more has been revealed and much has been learned about consumer data privacy practices. However, as revealed by Zatko in the summer of 2022, the technical expertise held by regulators is demonstrably lagging compared to highly

56. Mariam Baksh, *Whistleblower Explains How Twitter Easily Skirted FTC's Data Security Enforcement*, NEXTGOV/FCW (Sept. 14, 2022), https://www.nextgov.com/cybersecurity/2022/09/whistleblower-explains-how-twitter-easily-skirted-ftcs-data-security-enforcement/377130. The inadequacy of the SEC's whistleblower program for unfair or deceptive consumer data practices is discussed in Part IV. Generally, an insider is not eligible for a reward unless the SEC brings action. *See* 7 U.S.C. § 26(b)–(h) (setting forth whistleblower reward and protection requirements); 15 U.S.C. § 78u-6(b)(1) (discussing reward eligibility); 15 U.S.C. § 78u-6(a)(5) (including reward eligibility when there is a subsequent successful action "brought by an entity described in subclauses (I) through (IV) of subsection (h)(2)(D)(i)"); 15 U.S.C. § 78u-6(h)(2)(D)(i) (including "an appropriate regulatory authority"); SEC Rule 240.21F-4(g) (defining an "[a]ppropriate regulatory authority" as "an appropriate regulatory agency other than the Commission"); 15 U.S.C. § 78c(a)(34) (not mentioning the FTC).

57. Twitter, Inc., No. C-4316 (F.T.C. Mar. 2, 2011).

58. *Transcript*, *supra* note 9.

59. United States v. Twitter, Inc., No. 3:22-cv-3070, 2022 WL 1768852, at *1 (N.D. Cal. May 26, 2022).

60. *Transcript of Mark Zuckerberg's Senate Hearing*, WASH. POST (Apr. 10, 2018, 8:25 PM), https://perma.cc/7PFP-V3U5.

sophisticated commercial entities. More hurdles remain to bring a successful action with deterring effects.

C. The FTC's Enforcement Power Legal Process Is Also Procedurally Inefficient

Assuming an investigation is successful enough, the FTC then develops a record and takes legal action.[61] The FTC generally cannot seek civil (monetary) penalties in first actions against a company.[62] Rather, the FTC's first action against a particular company results in a court ruling imposing only equitable monetary remedies, or non-monetary imposed obligations.[63] Another option allows a company to preempt a court order and voluntarily enter into an agreement imposing obligations.[64] As mentioned above, typical FTC enforcement remedies require prohibiting acts complained of, remediating problematic acts, deleting wrongfully obtained information, modifying privacy policy, establishing a comprehensive privacy program, undergoing biennial audits, and adhering to record-keeping and reporting obligations.[65]

Even after an agreement becomes binding, thus leaving the company susceptible to civil penalties if found to be in violation of its agreement, there are still issues the FTC faces. The recent Twitter whistleblower case in the summer of 2022 illustrates one such problem.[66] The initial obligations imposed by the FTC after its first action against a company seek to foster a level of transparency and promote accountability through things like reporting requirements and audits.[67]

However, when Zatko testified in front of Congress about his experience working as Twitter's CSO, he revealed an unsettling reality: bound companies' reporting requirements are easily manipulated, leaving them with the ability to still practice unfair or deceptive practices without huge deterrence.[68]

61. *See* Solove & Hartzog, *supra* note 39, at 69.
62. *See supra* notes 38 and 39.
63. *See id.*
64. *See id.* at 610.
65. *See id.* at 614–18.
66. *See* Baksh, *supra* note 56.
67. *See* Solove & Hartzog, *supra* note 39, at 614–18.
68. *See* Baksh, *supra* note 56.

Zatko testified that Twitter did not admit to its systemic failure to delete consumer data when asked directly whether or not it did so in an interview by the FTC.[69] Instead, Twitter may have intentionally tried to mislead the FTC when it skirted the question and replied, "we deactivate users."[70] In reality, Twitter had not deleted user information.[71] Additionally, Zatko testified "third-party" FTC-required security certifiers were often hired by Twitter itself, indicating "a conflict of interest."[72] It was only through a whistleblower that the FTC eventually became aware of what was going on.[73]

The above discussion indicates the hurdles for the FTC are so numerous that their efficiency and deterrence is significantly hampered. A first action is effectively a warning, and though it has the potential for eventual huge consequences, companies recognize and take advantage of the uphill battle the FTC faces. As a result, companies have demonstrably found workarounds, see the risk-to-reward ratio as still heavily in their favor, and continue at least some of their unfair or deceptive practices with consumer data.

D. The FTC's Enforcement Power Can Be Inadequate, Resulting in Undeterred Companies with Compliers Facing Competitive Disadvantages

Aside from being inefficient, the FTC's enforcement power can also be inadequate. This could happen where actual harm has already occurred, and the FTC is only on its first action of enforcing with only non-punitive and equitable remedies available.[74] Companies are not deterred from ensuring consumer data is used and stored properly because of the FTC's level of inefficiency and inadequate remedies.[75] Without deterrence and with a lucrative alternative, prevalent risks to consumers' data follows.[76]

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*

73. *Id.*

74. *See supra* note 38.

75. *See The U.S. Urgently Needs a Data Protection Agency*, ELEC. PRIV. INFO. CTR., https://epic.org/campaigns/dpa (last visited Oct. 6, 2023) (discussing the failures of the FTC to enforce privacy laws).

76. *See id.*

Inconsistent investment in compliance can also create inequitable competitive disadvantages among companies.[77] This happens when businesses trying to comply invest significantly in compliance.[78] As a result, their data practices may become less lucrative.[79]

A competitive disadvantage can be further exacerbated because of the lack of clarity in what warrants unfair or deceptive trade practices in the data privacy context.[80] The FTC has yet to use its rulemaking power to articulate bright line requirements or exclusions.[81] Although an abundance of rulemaking can be overburdening,[82] a lean and efficient level of bright line rules would help point companies in the right direction for issues the companies must address.[83] Although companies can look to prior actions by the FTC in this context, some situations are uniquely fact-specific, and it is more difficult to discern how narrowly or broadly the precedent may apply.[84] A desirable example that would not impede innovation would include a bright line to make clear where there would be carveouts or exceptions. Without bright lines or articulated exceptions, the disadvantage to companies striving to comply increases relative to those that continue to capitalize on non-compliance or to those that put forth minimal efforts.[85]

77. This Note focuses on the federal enforcement by the FTC and does not discuss the regulation of consumer data privacy at the state level. However, inconsistent investment in compliance and overburdening companies due to conflicts among patchwork state laws is a common concern at the state level. *E.g.*, DANIEL CASTRO, LUKE DASCOLI & GILLIAN DIEBOLD, THE LOOMING COST OF A PATCHWORK OF STATE PRIVACY LAWS 12–16 (2022) https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws.

78. Trade Regulation Rule, *supra* note 16, at 51280.

79. *See id.*

80. Companies can be without clear notice because "[w]hat constitutes a deceptive or unfair trade practice has evolved, depending on what business practices the FTC has deemed problematic at any given time." Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 327 (2013).

81. *See* Trade Regulation Rule, *supra* note 16, at 51289.

82. A discussion of ex ante and ex post redress is discussed in Part IV. Specifically, an overly prescriptive approach with an abundance of bright line rules could be overburdening and hinder innovation because it would tend to assume a single set of consumer preferences or presume ways in which technology can or will evolve. The alternative, a broad ex ante approach, would scrutinize all possible data activities and violations in advance. It can also assume one general type of data preferences.

83. *See* Asay, *supra* note 80, at 327.

84. *See* Trade Regulation Rule, *supra* note 16, at 51280–81.

85. *See id.*

However, some might argue that the current level of inefficiency is acceptable and possibly desirable so that technological innovation may continue without being overly hindered.[86] This notion is rooted in the assumption that consumer data provides benefits to society at large that outweigh the level of current known harms resulting from inefficient data privacy regulation and enforcement.

A discussion of data privacy harms takes place below. It establishes that a lack of data privacy and security fostered by inefficient regulation enforcement has resulted in actual direct harms, grievous attenuated harm, and massive risks of additional kinds of known and lesser-known harm. The next Part reveals a hole and rebuts the above stated assumption that would prefer to promote the status quo: the argument for the status quo does not adequately give weight to the serious risk of not yet fully understood or seemingly attenuated harms. The following discussion furthers the notion that current inefficient enforcement is not acceptable, and that the proposed whistleblower incentive is needed. An incentive would promote efficiency and accountability, foster research and understanding, but refrain from over-burdening commercial interests.

III. KNOWN HARMS, LESSER-KNOWN HARMS, AND CHALLENGES IN ADEQUATELY ADDRESSING HARM

Addressing harm is difficult in the data privacy context. This is because being able to show legally cognizable harm is often a prerequisite for data privacy actions and an element for many causes of action.[87] This discussion broadly and briefly examines the range of harms from unfair or misleading consumer data practice and how those harms affect individuals, society, businesses, and national security. This is done to help explain important features of the proposed incentive.

First, there is a brief overview of known and concrete harms that result from a lack of data privacy. Second, there is a discussion about lesser understood harms that are difficult to cure through

86. Stephanie Comstock Ondrof, "*Senator, We Run Ads": Advocating for a US Self-Regulatory Response to the EU General Data Protection Regulation*, 28 GEO. MASON L. REV. 815, 848–52 (2021).

87. *See* Citron & Solove, *supra* note 12, at 796.

legal remedies but are important to understand and prevent. Third, this Part also discusses some of the good things happening in the data privacy context that can be further cultivated through the proposed incentive.

A. Known and Concrete Harms

"Harms involve injuries, setbacks, losses, or impairments to well-being[,]"[88] leaving people or society worse off. Regarding legally known and recognizable harm, data privacy breaches present tangible financial or physical harms ranging from mild to extreme.[89] Various forms of stalking from data breaches, improper collection, or data sales have led to multiple types of damages. These include death threats,[90] harassment,[91] "doxing,"[92] "swatting,"[93] and murder.[94] Data breaches from a lack of security or improper practices can also leave consumers more vulnerable to cyber-security threats, identity fraud, and theft, with financial repercussions ranging from slight to significant.

In November 2022, the FTC hosted its seventh annual PrivacyCon, where the harm of algorithmic bias was a key focus.[95] A panel on *Bias in Algorithms* presented researchers' findings:

88. *Id*. at 799.

89. *See id*. at 830–61.

90. *See Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists*, 290 F.3d 1058, 1065 (9th Cir. 2002) (en banc) (involving abortion doctors and their families receiving death threats).

91. See Citron & Solove, *supra* note 12, at 818; *see generally* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014) (providing an in-depth examination of the prevalence and extent of personal cyber-attacks, including harassment, and proposing practical, lawful ways to prevent and punish online harassment).

92. "Doxing" is a form of intimidation where data is revealed to help others in tracking a person down to attack, threaten, or otherwise harass them. *See* Ryan Goodrich, *What Is Doxing?*, TECH NEWS DAILY (Apr. 2, 2013) https://web.archive.org/web/20141029095609/http://www.technewsdaily.com/17590-what-is-doxing.html.

93. "Swatting" is a harassment practice that involves falsely calling in an emergency threat to law enforcement to send officials to an address. *See* Daniel J. Solove, *Data is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. U. L. REV. (forthcoming 2024) (manuscript at 36) [hereinafter Solove, *Data is What Data Does*].

94. An example of this is described in *Remsburg v. Docusearch*, 816 A.2d 1001 (N.H. 2003), a case which arose after a stalker bought a woman's work address from a personal data search company, then stalked and murdered her.

95. *See* Ziad Obermeyer, Brian Powers, Christine Vogeli & Sendhil Mullainathan, *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 AM. ASS'N FOR ADVANCEMENT SCI. 447, 447 (Oct. 25, 2022).

an algorithm used with the intentions of targeting medical interventions to the sickest patients ended up directing resources to a healthier, white population.[96] This same group of researchers established that black patients were sicker than white patients, with black patients needing an increase in help from 17.7–46.5% to alleviate the disparity.[97] This research is unsettling and indicates the prevalence of harms arising from the data collection and algorithms used in everyday life.

B. Issues with Less-Cognizable Privacy Harms

Although recognizable harms are potentially pervasive, data privacy harms more often involve injuries that are difficult to assign a monetary value to and are thus less legally recognizable. These injuries range from mild to monumental in either isolation or aggregation. For example, it would be difficult to quantify a monetary remedy for the mental anguish teen girls experience through Instagram flooding their feed with targeted squares displaying body image perfectionism. Even though an insider leaked research that showed Instagram made one in three teen girls feel worse about their bodies, the current legal scheme would

96. Algorithms and privacy are often treated as separate and distinct areas for regulation. Algorithms can include "design harms," which are considered separate and distinct from "privacy harms." To illustrate the difference, an Instagram or other camera application filter that uses teens' faces—making their faces appear to have bigger lips, eyes, etc.—can promulgate body dysmorphia. This could be considered a design harm. These filters can also be gamified to encourage sharing the filter with friends, expanding the impact. Alternatively, a privacy harm could exist in this same scenario where that same filter captures and stores the facial features of teens, tracks who the filter is shared with, and subsequently uses that data to further develop harmful products or promulgate ads with similar issues to vulnerable individuals. This example demonstrates that a privacy harm can exacerbate a design harm. Algorithms and artificial intelligence continue to develop by the data received and learned from. As such, algorithms present situations in which the data used could result in an area of overlap between a design and a privacy harm. An algorithm's use of consumer data could amount to a deceptive or unfair use of the collected data. This Note does not focus on design harms, however, for further discussion of the two and their overlap, see *Harmful Design in Digital Markets: How Online Choice Architecture Practices Can Undermine Consumer Choice and Control over Personal Information*, DIGITAL REGULATION COOPERATION FORUM, https://www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf (last visited Oct. 10, 2023).

97. Obermeyer et al., *supra* note 95, at 447.

struggle to quantify this harm on an individual basis.[98] On an aggregated scale, the harm is huge and the societal impact through its ripple effect is strong. But articulating legal restoration in cases like these is a practical struggle.

These harms are difficult to quantify but nonetheless carry consequences considered repugnant in other areas of the law. Broken contractual promises occur when consumers consent to company data privacy practices and companies stray beyond these condoned data uses. This also results in thwarted expectations about how people's data will be collected, used, disclosed, and traded. The downstream effects of the broken promises, thwarted consumer expectations, and unsanctioned data use have harmful consequences that are difficult to determine and often impossible to calculate.[99] The biased algorithms are just beginning to be understood and so are still somewhat incognizable at law. Harms range from unwanted spam or an eerie sense of surveillance to widespread discrimination, exacerbation of racial inequities, political manipulation, shame, embarrassment, ridicule, reputational humiliation, emotional distress, anxiety, and depression.[100]

Articulating "harm" in this context is difficult because some harms are developing, just like the technology the harms stem from.[101] One other fundamental reason may be best illustrated using an analogy to a once omnipresent and largely unregulated industry—the tobacco industry.

"Facebook seems to be taking a page from the textbook of Big Tobacco—targeting teens with potentially dangerous products while masking the science in public."[102] Tobacco was a substance that was initially unregulated, and its harms were largely not understood.[103] It was highly popular, highly lucrative, and even touted to be beneficial.[104] However, it was eventually discovered

98. *See* Georgia Wells, Jeff Horwitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sept. 14, 2021, 7:59 AM), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739; Citron & Solove, *supra* note 12, at 796–813.

99. *See* Citron & Solove, *supra* note 12, at 797.

100. *See id.*

101. *See id.* at 817–18.

102. Wells et al., *supra* note 98.

103. *Id.*

104. *See* Anne Charleton, *Medicinal Uses of Tobacco in History*, 97 J. ROYAL SOC'Y MED. 292, 292 (2004).

that tobacco has serious, proximate, and concrete harms.[105] Before thorough research and understanding, a harm like heart disease to smokers or eventual birth defects resulting from secondhand smoke exposure may have at first seemed too attenuated. But with more study, it eventually became clear these harms were directly linked to the consumption of tobacco.[106]

The important difference between data and drugs illustrates one fundamental problem in adequately addressing harm: Consumer data is unlike tobacco, because scientists could simply purchase and deconstruct a cigarette, then proceed to test its contents and effects in various ways. With data, private companies keep their data, inferences, algorithms, and hyper-specific uses under lock and key.[107] Because of this, harms are much more difficult to research, understand, and discover. As a result, many data privacy harms will continue to be without effective protections and remedies through the law.

Companies have developed restrictive policies on voluntarily sharing information.[108] Even if researchers went ahead and purchased consumer data from entities, researchers would still be unable to fully understand how it is used or what kind of correlations are possible without insight.[109] Researchers can only softly predict what correlations exist between the data, the amount of harm, and the types of harm that result.[110] Without insight, researchers and regulators lack the ability to develop a first-hand understanding or otherwise deconstruct the gathered data, its use, and its harms.[111]

Pressing questions to alleviate known issues cannot be answered without insight into companies' proprietary data. For example, are there patterns in how news outlets and social media companies filter, censor, or promote the news to consumers by ideology, race, or other discriminatory factors? How does consumer

105. *See id.*

106. Press Release, Center for Disease Control, Smoking Early in Pregnancy Raises Risks of Heart Defects in Newborns (Apr. 7, 2008).

107. *See* Mary D. Fan, *The Right to Benefit From Big Data as a Public Resource*, 96 N.Y.U. L. REV. 1438, 1438–92 (Nov. 2021) (discussing the value and benefit the public would have with a right to access collected data as a public resource).

108. *See id.* at 1443–44.

109. *See id.*

110. *See id.*

111. *See id.*

data influence or relate to the rise of violent extremism? How might consumer data be used to discriminate access to health care, employment, price-savings, or other opportunities?

The law's shortcomings in remediating, preventing, and even understanding harms are exacerbated because companies are without motivation to research concrete and less-cognizable harms. However, there are important instances where companies voluntarily gave insight to help solve societal issues.

C. Pieces of Positives to Build on in Data Privacy Law

There are instances of important, good things going on in the data privacy context that should continue to be incentivized and built on. For example, in 2020, Google voluntarily released free data sets to help teach machine learning how to help prevent the spread of COVID-19.[112] Additionally, Facebook and Social Science One released social science datasets to study elections and the spread of misinformation.[113] These are instances that should be incentivized and facilitated through the law. As for the regulatory system, the FTC has proven to be an important tool to help prevent potential data privacy damages. Incentives should foster companies coming forward with research that provides valuable benefits to society and diminishes consumer harms.

The FTC has a particular advantage in regulating consumer data because it does not have the requirement to establish harm for standing or damages.[114] For example, in October 2019, the FTC brought its first case against developers of "stalking" apps.[115] The apps were designed to run secretly in the background—with the ability to hide the app icon so a phone user would not know it was installed.[116] These apps were uniquely suited to illegal and

112. *See* Kyle Wiggers, *Google Cloud Releases Covid-19 Data Sets to Foster Coronavirus-Fighting AI Models*, VENTUREBEAT (Mar. 30, 2020, 9:39 AM), *https://venturebeat.com/2020/03/30/google-launches-covid-19-public-datasets-program-to-foster-coronavirus-fighting-ai-models*.

113. Gary King & Nathaniel Persily, *Unprecedented Facebook URLs Dataset Now Available for Academic Research Through Social Science One*, SOC. SCI. ONE (Feb. 13, 2020), https://socialscience.one/blog/unprecedented-facebook-urls-dataset-now-available-research-through-social-science-one.

114. *See* Citron & Solove, *supra* note 12, at 814.

115. *See* Retina A-X Studios, LLC v. James N. Johns, Jr., No. C-4711 (F.T.C. Oct. 2019).

116. *See id.*

dangerous uses.[117] The apps allowed purchasers to monitor the mobile devices on which the apps were installed, without the knowledge or permission of the device's user.[118] The case resulted in a settlement, aimed to resolve allegations that these apps "compromised the privacy and security of consumer devices on which they were installed."[119] Without the FTC's action, an ordinary consumer would have a difficult time proving monetary damages based on the app's information gathering alone without proof of monetary or other legally recognizable harm.

In sum, even though there are instances of progress, the argument for the status quo does not adequately give weight to the serious risk of not yet fully understood or seemingly attenuated harms. Nor does it account for the inability to better understand them. The current inefficient enforcement is not acceptable, and the proposed whistleblower incentive is needed. This is because it promotes efficiency and accountability, fosters research and understanding, and can prevent harm, but refrains from over-burdening or over-regulating commercial interests.

The next Part shows how a whistleblower incentive would offer unique solutions to an area of law that struggles to both recognize and remedy harm. Needed incentive traits are discussed below.

IV. CARROT CHARACTERISTICS

Incentives are an integral part of intellectual property law. For example, patent law works to discourage trade secrets by providing inventors with an incentive to publicly disclose their original and substantial inventions to the United States Patent and Trademark Office.[120] In exchange, if a patent is granted, inventors can secure exclusive rights to their discoveries for a limited time.[121] An incentive in data privacy law could facilitate commercial progress and discourage total trade secrecy by rewarding beneficial research

117. *See id.*

118. *See id.*

119. *USA: FTC Announces Proposed Settlement with Retina-X Studios for Tracking Apps*, DATAGUIDANCE (Oct. 23, 2019), https://www.dataguidance.com/news/usa-ftc-announces-proposed-settlement-retina-x-studios.

120. *See* Anderson, *supra* note 15, at 921.

121. *See* U.S. CONST. art. I, § 8, cl. 8; *see also* Wendy J. Gordon, *Intellectual Property*, *in* THE OXFORD HANDBOOK OF LEGAL STUDIES 617, 632 (Peter Cane & Mark Tushnet eds., 2003).

or access to data. An incentive would also remain rooted in the notion of protecting consumers.

This Part outlines and analyzes four necessary qualities of a whistleblower incentive relating to the FTC and consumer data privacy: it should (1) be narrow and only address unfair or misleading consumer data practices; (2) provide protection for whistleblowers with an avenue for remaining anonymous and prohibiting companies from retaliating against protected whistleblowers; (3) include clear-cut requirements for a whistleblower to be eligible for both protection and reward; and (4) include a mandatory reward when requirements are satisfied, with a specific range the reward amount will be based on. The supporting reasons for each of the above-listed characteristics are discussed below.

A. A Narrowly Tailored Incentive

First, a whistleblower incentive should be narrow and address only consumer data. Insiders would report to the FTC either (1) known deceptive or unfair data practices that would violate the law or a previously entered agreement with the FTC; or (2) practices that would likely be considered "deceptive" or unfair. The incentive should be tailored to this purpose for multiple reasons. Having a clear-cut and narrow incentive will provide certainty for tech workers as they go through their own complicated cost, risk, and ethical analysis.[122] This clarity helps tech workers know whether they would be protectable whistleblowers or potentially illegal leakers facing hefty financial liability or even criminal charges. Clarity and certainty also help fight other forms of deterrence from disclosure that tech workers must grapple with. Specifically, a potential whistleblower has real relationships with

122. There is a current bill in the House of Representatives, H.R. 6093, which proposes a broad whistleblower incentive for the FTC generally, but it has multiple flaws that will likely keep it from passing. Each of the characteristics discussed in this Note are largely not present in H.R. 6093. Introduced in November 2021, this bill is set to expire if not voted on within two years, by November 2023. Though not discussed further, the failure of this bill helps demonstrate that an incentive needs to be narrower. *See* H.R. 6093, 117th Cong. (2021) See *also* Dallas Hammer & Jason Zuckerman, *FTC Whistleblower Act Would Reward and Protect Whistleblowing About Data Privacy Misconduct and Other Deceptive Practices*, THE NATIONAL LAW REVIEW (Dec. 3, 2021), https://www.natlawreview.com/article/ftc-whistleblower-act-would-reward-and-protect-whistleblowing-about-data-privacy (analyzing the characteristics of H.R. 6093).

friends and colleagues at stake. A worker's reputation and career are also on the line because "[i]t's hard to find employment when you've been branded as the whistleblower."[123]

Additionally, the clear parameters will make things more manageable for the FTC by providing better quality insight. Funneling a whistleblower incentive to only data privacy will enable the FTC to develop a more focused, meaningful, and calculated response to the insight it receives. One important reason for a whistleblower incentive is to offer otherwise unavailable insight for policymakers to learn from. This focused insight will help the FTC as it develops and promulgates new rules. Insight and learning are needed to prevent an overly cumbersome number of rules from being implemented. Instead, learning more from companies will help regulators foster lean and efficient guidelines for what constitutes unfair or deceptive data practices. With the insight and resulting rules, the FTC will be able to improve its efficiency in significant ways.

Narrow parameters are also necessary to balance and pace the effects on the data industry. A moderate pace is ideal because an essential part of the FTC's purpose is to avoid unduly burdening legitimate business activity. Historically, the FTC has taken a stair-stepping and slow approach to developing its own sort of precedent.[124] This is done intentionally to give companies more notice of what is expected from them without requiring the FTC to go through a formal rulemaking process.[125] Further, a tailored incentive will also help companies conceal their otherwise legal trade secrets. This will help insiders limit what they disclose, which also helps promote commercial interests.

B. An Incentive with an Avenue for Anonymity and Protection

Second, a whistleblower incentive should provide protection by offering an avenue for anonymity to insiders. If anonymity is not chosen, there should be provisions prohibiting companies from retaliating against protected whistleblowers. Anonymity and

123. Bloch-Wehba, *supra* note 51 (manuscript at 30) (citing Kristian Hernandez, *COVID Underscores Lack of Whistleblower Protections*, STATELINE (Feb. 14, 2022), https://pew.org/3oHpHaR).

124. *See* Trade Regulation Rule, *supra* note 16, at 51273.

125. *See id.*

protection from retaliation are necessary to help alleviate some of the social costs involved that are outside of the civil, criminal, and professional liability. A real-life situation illustrates the need for such provisions below.

A leak by an Apple employee illustrates the stakes insiders face when forced with difficult ethical questions. An Apple employee leaked a memo posted on the company's internal blog.[126] Apple's memo offered statistics on employee leaks and enforcement.[127] It reminded workers that "[i]n 2017, Apple caught 29 leakers. 12 of those were arrested."[128] The memo also touted that the company was able to pinpoint and catch a single employee who leaked information from a meeting with hundreds of employees in attendance.[129]

Apple was not just attempting to ensure total trade secrecy; it was intimidating employees by threatening that it would take criminal action against employees who leaked insider information. In addition to criminal penalties, Apple's employees would also face legal and social consequences. Insider insight is needed in an information imbalanced system, but the stakes are high.

Protection from professional retaliation is also needed because the foundation of at-will employment allows employers to fire their employees "for what [employees] say" or for most other reasons.[130] Additionally, the constitutional freedom of expression is not enough to protect private-sector employees from their "voluntary" non-disclosure agreements (NDAs) or other acceptable employment practices.[131]

Further, without retaliation protections, whistleblowers could face both civil and criminal liability. Freedom of contract often prevails over freedom of employee speech. Contracts are used to

126. *See* Mark Gurman, *Apple Warns Employees to Stop Leaking Information to Media*, BLOOMBERG (Apr. 13, 2018, 11:18 AM), https://www.bloomberg.com/news/articles/2018-04-13/apple-warns-employees-to-stop-leaking-information-to-media.

127. *See id.*

128. *Id.*

129. *Id*.

130. *See* Bloch-Wehba, *supra* note 51 (manuscript at 15) (quoting Charlotte Garden, *Was It Something I Said?: Legal Protections for Employee Speech* 1, ECON. POL'Y INSTITUTE (2022)).

131. Bloch-Wehba, *supra* note 51 (manuscript at 16); *see also* Pauline T. Kim, *Market Norms and Constitutional Values in the Government Workplace*, 94 N.C. L. REV. 601, 610 (2016).

restrict trade secrets. An employee divulging trade secrets can face criminal charges in some instances.[132]

Employee NDAs can also extend beyond legitimate trade secrets to broadly defined "confidential information."[133] Even when employers know their NDAs are so overbroad that they are legally unenforceable, companies use them anyway. This is because employees are still deterred from going anywhere close to a line that would cause legal complications from an NDA.[134]

Whistleblowers also need protection because even if they want and try to remain anonymous, there is a legitimate chance whistleblowers will get caught by their company. As the example of Apple's internal memo illustrates, companies are good at catching employee leaks due to a broad use of workplace surveillance. Companies prioritize intense investigative efforts to catch and punish leakers. Without some level of protection, whether there is a reward on the line, the numerous risks and costs employees would otherwise face will almost always outweigh their desire and ability to inform the public, academics, and regulators of wrongdoing.

C. An Incentive with Clear-Cut Requirements for Reward and Protection Eligibility

Third, a whistleblower incentive should include clear-cut requirements and exclusions for an employee to be eligible for both protection and reward. Some ideal requirements and exclusions would include:

- An FTC Whistleblower must voluntarily provide original information relating to a possible violation of a business conducting unfair or deceptive consumer data practices.
- This insight must lead to the successful enforcement by the FTC of a federal court or administrative action in which the FTC obtains monetary sanctions totaling more than one million dollars.

132. *See* 18 U.S.C. §§ 1831–39; *see also* Madeleine Cane, Michael Bednarcyzk, Maxwell Nides, Patrick Engle & Quinlan Cummings, *Intellectual Property Crimes*, 58 AM. CRIM. L. REV. 1151, 1154–55 (2021).

133. Orly Lobel, *NDAs Are Out of Control. Here's What Needs to Change*, HARV. BUS. REV. (Jan. 30, 2018), https://hbr.org/2018/01/ndas-are-out-of-control-heres-what-needs-to-change.

134. *See id.*

- Whistleblowers would still be eligible for a reward if they first report internally and the company informs the FTC about the violations.
- Certain people would not generally be eligible for rewards, including people who have pre-existing legal or contractual duties to report their information to the FTC, such as attorneys, compliance personnel, and internal auditors.
- To fall under the FTC's employer anti-retaliation protection, the whistleblower must possess a reasonable belief that the information that the whistleblower provides relates to a possible FTC violation that has occurred, is ongoing, or is about to occur.

Different schools of thought provide legitimate reasons for the clear-cut protection and reward eligibility requirements. As established in the discussion of the FTC's shortcomings, there is a legitimate need to help with enforcement because the FTC is without sufficient human-capital, monetary-capital, and lacks technological detection ability.[135]

There is also a conceptual regulatory need. The FTC's current actions do not create bright-line precedent to follow:[136] Instead, clearer regulations should be formed to synthesize and streamline the holdings of FTC caselaw. Whistleblowers will help point regulators in the right direction of problems. This gives regulators insight on common problems, how to create clearer rules, and where exceptions need to be expressly carved out.

Clear-cut protection and incentive requirements are also desirable because such requirements are already proven to work in other areas of law—namely, securities violations. However, the SEC's whistleblower laws do not fully cover unfair or deceptive data practices. Data practices are largely outside the SEC's enforcement power and are instead within the FTC's jurisdiction. The specifics are discussed below.

The SEC's Dodd Frank Act helps show that incentives are a proven method.[137] Since 2010, whistleblower tips have helped the SEC to recover nearly $5 billion in monetary penalties, with $1.3

135. *See* Bloch-Wehba, *supra* note 51 (manuscript at 50–51).

136. *See* Solove & Hartzog, *supra* note 39, at 585–86.

137. *See* 7 U.S.C. § 26(b)–(h) (setting forth whistleblower reward and protection requirements).

billion in investor restitution.[138] These instances would likely be undiscoverable without a whistleblower pointing a finger in the right direction. The Commodities Futures Trading Commission (CFTC) is an additional example of an agency with a successful whistleblower program.[139] The CFTC issued its first reward from its Whistleblower Program in 2014 and has since granted several whistleblower awards, which have led to cumulative monetary sanctions of more than $3 billion.[140]

The SEC's whistleblower program also establishes that there are other reasons for an FTC whistleblower program regarding unfair or deceptive data privacy practices. This is because there are already important instances where tech workers, in the absence of specific data privacy whistleblower protections, have innovatively situated themselves to fall within the SEC's whistleblower protection laws.[141] In some of these instances, the FTC used information gained through the whistleblowers' leaks to the SEC to subsequently bring successful FTC actions against the companies. However, although helpful for the FTC and for insiders seeking protection, the SEC's whistleblower laws are not an obvious route to protection for insiders when it comes to data security. Without a clear path and relatively certain protections, the vast majority of appropriate insider insight will remain chilled. A narrow FTC whistleblower incentive and protection, on the other hand, would make things clearer and facilitate appropriate insight.

It also seems that an SEC whistleblower would not be eligible to recover any monetary bounty where only the FTC brings subsequent successful action. This is because the FTC is not listed under the SEC's laws that articulate the requirements for a whistleblower to be eligible for a reward.[142] There is no mention of

138. SEC. & EXCH. COMM'N, SEC ANNUAL REPORT TO CONGRESS: WHISTLEBLOWER PROGRAM 1 (2021).

139. *See id.*

140. Press Release, Commodities Futures Trading Commission, CFTC Awards Approximately $10 Million to a Whistleblower (Mar. 18, 2022).

141. *See supra* Section IV.A.

142. *See* 15 U.S.C. § 78u-6(b)(1) (discussing reward eligibility); 15 U.S.C. § 78u-6(a)(5) (including reward eligibility when there is a subsequent successful action "brought by an entity described in subclauses (I) through (IV) of subsection (h)(2)(D)(i)"); 15 U.S.C. § 78u-6(h)(2)(D)(i) (includes "an appropriate regulatory authority"); SEC Rule 240.21F-4(g) (defining an "[a]ppropriate regulatory authority" as "an appropriate regulatory agency other than the Commission"); 15 U.S.C. § 78c(a)(34) (not mentioning the FTC).

the FTC or use of sweeping terminology that would otherwise qualify the FTC in the SEC's rules defining "appropriate regulatory agency" or "appropriate regulatory authority."[143] Thus, an FTC whistleblower incentive would again provide a more certain and clear path for insiders.

D. An Incentive with a Mandatory and Specific Reward Range

Fourth, a whistleblower incentive should, when requirements are satisfied, include a mandatory (as opposed to discretionary) reward with a specific range that the reward amount is based on. This point pairs with the benefits of clear lines and ease of risk analysis discussed in Part III; however, there is an additional important reason for mandatory rewards. Imposing mandatory rewards where requirements are met means the FTC would recover and benefit from monetary penalties. With the incentive in place and assuming a higher volume of successful enforcement actions, the FTC's portion of the recovery could be used to help fund its inadequate resources.

With these characteristics in mind, the next Part delves into eight benefits a narrow FTC whistleblower incentive would provide, including important ways it would improve deficiencies and inadequacies in the current FTC enforcement and regulatory system.

V. EIGHT ADVANTAGEOUS BITS OF THE CARROT BYTE

Tech leaks have already established their value and their necessity. Leaks have unearthed some of the most significant technology policy issues in the current landscape. Without these leaks, some important issues could have remained only suspicions and virtually undiscoverable. The uncovered issues' ripple effects have prompted federal regulatory action by the FTC, spurred congressional committees to convene,[144] and helped facilitate state efforts to get involved.[145] A few examples are included below.

143. *See id.*

144. *See* Bloch-Wehba, *supra* note 51 (manuscript at 23).

145. *See* Allison Slater Tate, *Facebook whistleblower Frances Haugen says parents make 1 big mistake with social media*, TODAY (Feb. 7, 2022, 5:06 PM), https://www.today.com/parents/teens/facebook-whistleblower-frances-haugen-rcna15256; Press Release, Utah Gov., Utah Sues TikTok Over Child Addiction Harm, Targets "Enmeshment" With Its China-Based Parent Company (Oct. 10, 2023), https://governor.utah.gov/2023/10/10/utah-sues-tiktok-over-child-addiction-harm-targets-enmeshment-with-its-china-based-parent-company.

In one notable example, Christopher Wylie, a former Cambridge Analytica employee, revealed how his company was using a new version of political campaigning through psychological targeting. His insight exposed that hundreds of thousands of users were lured to take a personality test—being paid to do so—and agreed to having their data collected and analyzed for "academic use."[146] The app "thisisyourdigitallife" was the test's platform. The app harvested data from both its users and their friends. At that time, Cambridge Analytica was run by Trump strategist Steve Bannon, and the company "used the harvested data to target [app] users with political advertising."[147] Although there was already suspicion surrounding Cambridge Analytica and Facebook's inappropriate data use and political targeting, both companies had been actively undermining such claims. The companies instead claimed nothing inappropriate had occurred and did not admit to exploiting collected user data without users' knowledge on behalf of political candidates. Without Wylie's leak that included supporting evidence, the suspicions could have dissipated and been disregarded.

Regarding election fraud and misinformation, Facebook leakers used company documents to establish that numerous employees repeatedly tried to raise red flags about misinformation spreading and conspiracies gaining traction before and after the contested November 2020 presidential election.[148]

In a separate instance, after Facebook allegedly dissolved its civic integrity team, a Facebook insider began taking the steps to intervene.[149] A Facebook insider facilitated a groundbreaking story by disclosing tens of thousands of internal Facebook documents to Congress and the Securities and Exchange Commission (SEC).[150] Another insider shared Facebook's research that revealed unsettling

146. Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

147. Bloch-Wehba, *supra* note 51 (manuscript at 36).

148. Ryan Mac & Sheera Frenkel, *Internal Alarm, Public Shrugs: Facebook's Employees Dissect Its Election Role*, N.Y. TIMES (Oct. 25, 2021), https://www.nytimes.com/2021/10/22/technology/facebook-election-misinformation.html.

149. Billy Perrigo, *Inside Frances Haugen's Decision to Take on Facebook*, TIME MAG. (Nov. 22, 2021), https://time.com/6121931/frances-haugen-facebook-whistleblower-profile.

150. *Id*.

statistics demonstrating that "[t]he tendency to share only the best moments, a pressure to look perfect and an addictive product can send teens spiraling . . . ."[151]

Other tech giants have had similarly important leaks. After a Google executive side-stepped a critical question in his congressional testimony, Google leakers helped break the news that the company was developing a censored search engine for China.[152] With these notable examples in mind, this next Part delves into eight separate benefits a narrow FTC whistleblower incentive would provide.

A. This Incentive Would Provide a Balanced Approach to Policymaking

First, a carrot and its characteristics provide a palatable policy balance because it would not limit either the direction of industry innovation or the options available to consumers. The incentive provides a balanced policymaking approach because an incentive combined with the FTC as an enforcer would be a type of ex post redress. Ex post redress means unfair or deceptive data practices are reviewed and fines or other penalties are put into place after they have occurred.[153] An ex post redress refrains from becoming an "overly prescriptive approach that assumes only one set of [consumer] preferences . . . ." Nor would an incentive "presume[]. . . ways in which technology can [or will] evolve."[154] However, it would still facilitate authority intervention in a more efficient way when necessary to prevent harm.[155]

The alternative, a broad ex ante approach, would "scrutiniz[e] all . . . possible data activities and violations in advance." An ex ante approach can also assume one general type of data preferences. One example of a prescriptive ex ante approach is Europe's General Data Protection Regulation (GDPR), which has resulted in some products, like email management and online game

151. Wells et al., *supra* note 98.

152. Alexis C. Madrigal, *Silicon Valley Sieve: A Timeline of Tech-Industry Leaks*, THE ATLANTIC (Oct. 10, 2018), https://www.theatlantic.com/technology/archive/2018/10/timeline-tech-industry-leaks/572593.

153. *See* Jennifer Huddleston, *A Primer on Data Privacy Enforcement Options*, AM. ACTION F. (May 4, 2020), https://www.americanactionforum.org/insight/a-primer-on-data-privacy-enforcement-options/#ixzz7xD3qbjBT.

154. *Id.*

155. *Id*.

applications, becoming unavailable in Europe "due to the cost or even impossibility of compliance" with the GDPR.[156] Although the ex post approach alone may not be enough, it could help ensure any type of incorporated ex ante approach remains lean and efficient.

B. This Incentive More Directly Addresses Data Use, Harms, and Risk of Harms than the Current "Sensitive Data" Approach

Second, this incentive offers an enforcement tool to directly address use, harms, and risks of harms more efficiently than the FTC is currently able to. In Professor Daniel J. Solove's forthcoming article titled *Data is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, Solove thoroughly addresses fundamental flaws with the current popular prescriptive approach that is framed around regulating "sensitive data."[157] In sum, he argues that regulations prohibiting broad and inconsistently defined "sensitive data" are unworkable for companies, counterproductive to innovation, and still pose serious risks of harms to consumers.[158]

The risks of harm remain due to notable omissions in sensitive data definitions, proxies that carry out harm without using "sensitive data," and because harmful algorithmic inferences based on "non-sensitive data" are highly accurate and proven to exist.[159] Instead, Solove argues for a system that would more directly address use, risk, and harm, and he notes the difficulty in this task.[160] He mentions a need for regulators to implement an approach that is proportionate to use, risk, and harm instead of a blanket approach with inconsistent definitions that have unclear boundaries.[161]

By being primarily geared toward an ex post redress, the incentive would give insight that could be evaluated based on the data's actual use. This would enable enforcement that is proportionate to the use of the data relating to harm or risk of harm. It would avoid creating a blanket approach that could otherwise

156. *Id.*

157. *See* Solove, *Data is What Data Does*, *supra* note 93.

158. *Id.*

159. *Id.* (manuscript at 33–43).

160. *Id.* (manuscript at 43–49).

161. *See id.* (manuscript at 29–30; 43–48).

treat uses disproportionately to their harm or risk of harm. This approach to addressing risk of harm also fosters a hybrid between an ex post facto and ex ante methodology. This is because regulators will gain valuable insight, learn from it, build on their expertise, and be in a better position to craft lean ex ante regulations. Equally as important, the incentive fosters enforcement by the FTC that would enable regulators to address harms no matter what type of data is used. Each of the later points of this Part address other inefficient aspects the FTC faces that were discussed in Part I.

Using the FTC to regulate harm in data privacy has another distinct advantage because actual harm is not a requirement for the FTC to have standing.[162] This removes the hurdle of having to show harm in a system that struggles with adequately addressing injuries in the data privacy context. The proposed whistleblower incentive would not change the way the FTC brings actions. As a result, a whistleblower incentive would not overreach into addressing harms that the system is not yet built to address, nor would it overburden commercial interests.

C. The Incentive Would Help Level the Current Data Information Imbalance, Inform Future Policymaking, and Easily Integrate into the Current System

Third, this incentive would be a counterweight to help balance the highly secretive nature of data information flow in a lagging regulatory system.[163] As discussed in section II(B), detectability is a major issue in determining when to bring initial actions, knowing where to look in investigations, understanding the evidence and technology being investigated, and keeping companies accountable to their subsequent settlement agreements. An incentive would facilitate insider insight that could provide valuable detection and evidence that is otherwise difficult to acquire. Also, where regulators are ill-equipped to fully understand what they are evaluating, whistleblowers can supply understanding and point regulators in the right direction.

162. *See* Asay, *supra* note 80, at 327 (citing PETER SWIRE & SOL BERMANN, INFORMATION PRIVACY 70 (2007)).

163. *See* Bloch-Wehba, *supra* note 51 (manuscript at 1).

Companies would also be less inclined to manipulate their answers to skirt liability throughout investigations.

Fourth, this incentive presents a palatable piece for the FTC to build on and learn from as the FTC confronts challenges in rulemaking. According to one report released by the agency, the FTC has brought more than 130 spam and spyware cases, 80 general privacy cases, 70 data security cases, and 100 cases involving Fair Credit Reporting Act violations.[164] Because of its extensive experience and congressional authority, the FTC is best situated to develop formal rules that create a balanced approach to consumer data privacy. A whistleblower incentive would provide an avenue for further insight, learning, and development. In the long run, by providing insight to the FTC and to Congress, regulations can be refined and adapted to better address risks and prevent injuries.

Fifth, a narrow incentive can be easily grafted onto any current or future "bundle of sticks" regulations. This advantage is straightforward and somewhat simple, but it should not be understated. Without cohesive federal laws that preempt patchwork state data privacy laws, adding any data privacy federal regulation quickly gets complicated even before considering politics. A whistleblower incentive would not add more regulations but rather would be used to assist current and future regulatory enforcement.

D. The Incentive Would Foster Transparency, Encourage Consistent Company Investment in Conformity, and Ultimately Promote Deterrence in an Efficient Way

Sixth, a whistleblower incentive could uniquely promote transparency and foster a better understanding of harm. Companies who might face liability as a result of a whistleblower could combat an extent of that liability by first making research of data use and its harms a priority; and second, by either making that research accessible to some level of outsiders or by allowing regulators, academics, and scientists to perform their own research with companies' gathered data. By doing this, the FTC and courts could take these acts into consideration when determining the extent of obligations imposed through settlement agreements or the amount sought in punitive recovery.

164. FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2019 (2019).

Seventh, the incentive encourages consistent investment by companies in implementing fair consumer data practices and following regulations. As discussed in Part II, the current lack of deterrence can create inequitable competitive disadvantages among companies and advantages for non-compliers. There are general principles that can be synthesized through the "precedent" created from previous FTC actions.[165] However, without clear rules and definitions, companies striving to comply can face hefty costs interpreting and complying with FTC precedent. With the threat of protected informants who are incentivized to come forward with a reward, companies will take their data privacy practices more seriously and make proper practices a priority. This incentive will bring equity where competitive disadvantages arise. Also, over time, the FTC will be able to bring more clarity to what warrants unfair or deceptive trade practices in the data privacy context through rulemaking and exclusions or consistent case law.

Eighth, a whistleblower incentive offers a way to promote deterrence without pumping more capital into enforcement agencies. As discussed in Part II, the FTC faces inadequate funding and minimal human capital to the point that it cannot facilitate a desirable amount of deterrence. This undermines its efficiency and ability to address harms. A whistleblower incentive would promote deterrence without more capital in multiple ways. Put simply, companies would be more deterred because the risk of FTC actions would go up. The incentive could also help fund the FTC, working to alleviate its lack of resources. This would be done by using part of the monetary penalties recovered to reward the whistleblowers and also to go either directly to the FTC, the U.S. Treasury, or all three.

The next Part confronts the potential disadvantages of a narrow incentive approach to helping the FTC. Ultimately, the next Part demonstrates that the incentive's benefits outweigh its drawbacks and that the incentive would not impede the commercial industry in a disproportionate way.

VI. DRAWBACKS OF THE INCENTIVE

While it would be convenient if a narrow FTC incentive surrounding consumer data privacy brought nothing but benefits,

165. *See* Solove & Hartzog, *supra* note 39 at 627–66.

there are potential drawbacks. Six main disadvantages are discussed below. Following each are considerations that rebut these concerns.

First, incentives used to facilitate wrongdoing can become an avenue for opportunism, over-incentivizing disclosure.[166] This carries a risk that employees might divulge conduct that is not particularly severe. Though this is a legitimate concern, overzealous claimants would still be part of a system full of checks and balances. The FTC would maintain discretion to determine whether the claims carry enough merit to bring an action. Further, the FTC would still be unable to seek monetary penalties until after a company breaches a previously entered settlement agreement. This ensures a slower pace of punishment. Also, a reward to any claimant is not a complete guarantee because there would be numerous requirements before a reward could be possible. Insiders would also still face a great amount of reputational risk outside of employer retaliation, which would deter those with imbalanced priorities.

Second, the law recognizes the importance of trade secrecy to innovation and capitalism, but this incentive could potentially play a part in destroying important proprietary information. This would happen by trade secrets becoming generally known. However, if the incentive is crafted correctly, and if insiders follow the steps to remain within its protections, insight would be given only to the FTC, meaning it would not be revealed to the media or other competitors. Further, the requirement that the insider hold a reasonable belief that the provided information relates to a possible FTC violation also helps filter out legal trade secrets from being disclosed. In sum, legal proprietary information would not easily become generally known, thereby destroying trade secrecy. Instead, only the necessary information to convey unfair or deceptive practices that are against the law would be included in publicly available information. This means that companies would still maintain legal trade secrets.

Third, the threat of employees becoming incentivized watchdogs could chill innovation. This is because companies may compartmentalize instead of collaborating, thus holding trade secrets within separate sectors to minimize potential oversight and liability. Cutting off collaboration would likely chill innovation.

166. *See* Bloch-Wehba, *supra* note 51 (manuscript at 43).

Yet this incentive is tailored much more narrowly than whistleblowing incentives already in place by the SEC, which have withstood the test of time and allowed society to continue innovating and advancing at an unprecedented pace. Additionally, incentives can be constructed to facilitate internal alerting and internal resolving before the FTC would otherwise get involved. Finally, there is a legitimate argument that not all innovation is good innovation, and it is okay for some of it to be chilled.[167] If companies sequester themselves to the point that their innovation is inhibited because their data practices are questionable, impeding this type of innovation might not be a bad result.

Fourth, some may argue the opposite problem of over-incentivizing: very few individuals actually blow the whistle to outside sources, because, as discussed above, such individuals face numerous drawbacks with high stakes.[168] However, with carefully implemented characteristics, anonymity and protections could alleviate these risks. Additionally, the incentive would not be intended to solve every problem and detect every issue for the FTC. It would only be one piece in enforcement meant to play an important but limited role in efficiently deterring wrongdoing. As previous examples demonstrate, insight from a small number of people can go a long way.

Fifth, "reactive lawmaking [alone] may . . . miss important opportunities for legal development and change."[169] However, it is important to remember that this proposed incentive is only one piece of a complex puzzle. A single incentive is not a one-size-cure-all type of solution. Nevertheless, this one piece could help regulators in the long run slowly shift from almost entirely reactive lawmaking to including some small pieces of law that are more prescriptive. A whistleblower incentive would help foster a better understanding of issues to help shape rulemaking by the FTC. This happens during the investigation process. With investigations, the FTC builds on its expertise and will begin to see firsthand what practices are prevalent, what harms are more likely, and what technologies are in play. With this new access to knowledge, regulators will be better informed to bring benefits to society.

167. *See* Stephanie Plamondon Bair, *Innovation's Hidden Externalities*, 47 BYU L. REV. 1385 (2022).

168. *See* Bloch-Wehba, *supra* note 51 (manuscript at 43).

169. *Id.* (manuscript at 45).

CONCLUSION

The status quo of the federal consumer data privacy law landscape is untenable. Society-shaping harms are at stake. Harms resulting from data privacy pitfalls are promulgated through inefficient enforcement, a lack of technological understanding, unclear legal lines, and data practices that are largely left without ethical oversight. Industry leaders and the public have called for a change, but an information imbalance between highly sophisticated companies and the lagging regulatory system has left lawmakers scratching their heads. However, at this point, an entirely prescriptive approach with such imbalanced technological understanding could overly hinder innovation by presuming how technology will evolve.

Balanced incentives are proven methods in areas of the law where trade secrecy combined with wrongdoing creates near-impossible detection. A narrow incentive with carefully crafted characteristics will help improve the status quo in numerous important ways. It would point the FTC in the right direction as it digs deep for deceptive data practices, learning and leveling the information imbalance along the way. Innovation would still flourish, and ex post enforcement would proportionately address data use to its harm. Proper data practices would become a priority, and companies would be motivated to be more transparent to limit their liability.

In sum, if left untilled and untouched, data privacy violations pose grave risks of harm to society. This Note's proposed incentive is the most realistic opportunity to impactfully address many systematic deficiencies in the current consumer data privacy landscape.