BROKERING SAFETY

Chinmayi Sharma,[*] *Thomas E. Kadri*[**] *& Sam Adler*[***]

For victims of abuse, safety means hiding. Not just hiding themselves, but also hiding their contact details, their address, their workplace, their roommates, and any other information that could enable their abuser to target them. Yet today, no number of name changes and relocations can prevent data brokers from sharing a victim's personal information online. Thanks to brokers, abusers can find what they need with a single search, a few clicks, and a few dollars. For many victims, then, the best hope for safety lies in obscurity—that is, making themselves and their information harder to find.

This Article exposes privacy law's complicity in this phenomenon of "brokered abuse." Today, victims seeking obscurity can ask data brokers to remove their online information. But a web of privacy laws props up a fragmented and opaque system that forces victims to navigate potentially hundreds of distinct opt-out processes, wait months for their information to be removed, and then repeat this process continuously to ensure their information doesn't resurface. The status quo compels victims to manage their own privacy, placing the burden of maintaining obscurity on already-overburdened shoulders.

In response, this Article pitches a new regulatory regime premised on a transformative reallocation of responsibility. In short, it proposes a techno-legal system that would enable victims to obscure their information across all data brokers with a single request, redistributing the burden away from victims and onto brokers. Such a system is justified, feasible, and constitutional—despite what brokers might say. The industry is eager to assert that it has a First Amendment right to exploit people's data, but this Article develops a trio of arguments to confront this controversial claim of corporate power. By blending theory, policy, and technical design, this Article charts a path toward meaningful privacy protections for victims and, ultimately, a more empathetic legal landscape for those most at risk.

[*] Associate Professor of Law, Fordham Law School.

[**] Assistant Professor, University of Georgia School of Law; Affiliate Faculty, University of Georgia Institute for Women's Studies; Legislative & Policy Director, Clinic to End Tech Abuse at Cornell University.

[***] J.D. Candidate, Fordham Law School. For feedback on earlier versions of this project, we thank RonNell Andersen Jones, Elettra Bietti, Hannah Bloch-Wehba, Ryan Calo, Ignacio Cofone, Julie Cohen, Amy Gajda, Yael Grauer, Nikolas Guggenberger, Woodrow Hartzog, Mike Hintze, Leigh Honeywell, Ido Kilovaty, Anne Klinefelter, Mark Lemley, Lyrissa Lidsky, Christopher Morten, Mark Nottingham, Paul Ohm, Natalia Pires de Vasconcelos, Chris Riley, Ani Satz, Evan Selinger, Scott Skinner-Thompson, Eugene Volokh, Rachel Vrabec, Ari Waldman, George Wang, Rebecca Wexler, and Felix Wu, as well as other participants at the Privacy Law Scholars Conference, UGA-Emory Faculty Workshop, and University of North Carolina School of Law Faculty Workshop. Authors are listed from most to least Kafkaesque.

TABLE OF CONTENTS

INTRODUCTION

Ella was in college when the abuse began.[1] She dated Nick for a while before trying to end their relationship. At that point, he "turned rather obsessive, showing up at my school, then showing up at my work." Before long, he came to her home to threaten her. She went to the police but wasn't taken seriously. Then things escalated. Nick showed up with a weapon. "I was almost killed." What stood between her and almost getting killed again? A few dollars and a few clicks on the internet. This is the plight of brokered abuse—the phenomenon of how data brokers enable and exacerbate stalking, harassment, and violence.[2]

Ella had left her abusive relationship, sought help, and fought for a restraining order. But none of that protected her when her abuser could still track her. "I'm not sure how, but [he] found information for my parents and made threatening calls to [them] as well. . . . [W]e knew it was him, but we were never able to do anything about it." With police unwilling or unable to intervene, Ella tried to erase herself—a defense mechanism that victims of brokered abuse know all too well. She abandoned the internet, moved cities, and changed her name, number, and career. And yet every time she tried to rebuild her life, her stalker found her again. The terror of knowing that digital breadcrumbs could lead him back to her consumed her. "If I Google my name and I'm showing up on Whitepages, People Finder, Spokeo, TrueIdentity—the list goes on and on and on—it's scary." Scrubbing her data became a constant, exhausting necessity. "This act of shielding myself became part of my everyday life."

Unfortunately, Ella's story is not unique. Countless others are trapped in cycles of fear and vigilance, their safety undermined by the ruthless machinery of the data-broker economy.[3] Data brokers are entities that collect personal information from public records, such as voter registrations and court filings, as well as private sources, including online purchases, social-media activity, and GPS location data.[4] They use this information to create comprehensive dossiers, detailing intimate aspects of individuals' lives—addresses, phone numbers, financial histories, family relationships, and more.[5] Brokers then sell these dossiers to businesses, government agencies, and even individuals.[6] The entire industry thrives on eliminating obscurity, systematically dismantling the practical difficulty of accessing and compiling personal information.[7] Victims like Ella are not seeking obscurity for the sake of secrecy but rather as a matter of safety and wellbeing. Yet the data-broker economy finds what is hidden, fueling cycles of interpersonal abuse.

---

1. Interview with Ella (May 31, 2022) [hereinafter Ella Interview]. All subsequent quotes and statements related to Ella's story are from this interview and will not be cited repeatedly for readability. To protect her anonymity, Ella is a pseudonym.

2. Thomas E. Kadri, *Brokered Abuse*, 3 J. FREE SPEECH L. 137 (2023).

3. *See, e.g.*, Kaveh Waddell, *How FamilyTreeNow Makes Stalking Easy*, ATLANTIC (Jan. 17, 2017), https://www.theatlantic.com/technology/archive/2017/01/the-webs-many-search-engines-for-your-personal-information/513323.

4. *See* Margaret B. Kwoka, *FOIA, Inc.*, 65 DUKE L.J. 1361, 1376–1401 (2016); David E. Pozen, *Transparency's Ideological Drift*, 128 YALE L.J. 100, 125 (2018); Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REGUL., 667, 669 (2017).

5. AMY GAJDA, SEEK AND HIDE: THE TANGLED HISTORY OF THE RIGHT TO PRIVACY 231–41 (2022); Andy Z. Wang, *Network Harms*, 91 U. CHI. L. REV. 2093, 2094–95 (2024).

6. Chris J. Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. 595 (2003).

7. *See* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343 (2015); Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way to Think About Your Data Than 'Privacy'*, ATLANTIC (Jan. 17, 2013); *see also infra* Part I.

The harms inflicted by data brokers are twofold: primary and secondary.[8] Primary harms arise from the immediate danger victims face when their personal information is exposed.[9] For victims like Ella, the knowledge that their abuser can easily track their movements, find their home, or access their contact details creates a constant state of fear and vulnerability. Despite the many steps Ella took to disappear, she could not escape the reach of data brokers who repeatedly exposed her location. This persistent threat can force victims to withdraw from social, professional, and community life, sacrificing opportunities and relationships in an effort to stay safe.[10]

Beyond these primary harms, victims endure secondary harms as they attempt to protect themselves in a broken system. The fragmented and opaque processes required to remove information from broker databases are arduous and retraumatizing.[11] Victims must locate and contact hundreds of brokers, verify compliance, and continuously monitor whether their data resurfaces.[12] Each step exacts an emotional and financial toll, forcing victims to revisit their trauma and confront the very systems that profit from their exposure.[13] These secondary harms compound the suffering of victims, making it clear that the status quo not only fails to protect them but actively deepens their pain.

The law is complicit in these harms. The American legal tradition of individual rights has left an indelible mark on American privacy law.[14] Today's privacy landscape defaults to a system of privacy self-management that Daniel Solove critiques as both unrealistic and inequitable.[15] Privacy self-management assumes that individuals can and should navigate complex systems to manage their own privacy, making informed choices about how their data is collected, stored, and shared.[16] While this concept aligns with a legal tradition rooted in individual rights and personal autonomy, it falls woefully short in the face of today's sprawling data ecosystems. Building on Solove's work, Ella Corren has effectively shown that privacy self-management places an impossible burden on individuals, offering an empirical rebuttal to the presumption that people have the resources, expertise, and bandwidth to make meaningful decisions about their privacy.[17] For victims of brokered abuse, this framework is especially harmful. It forces them to bear the weight of achieving obscurity, navigating labyrinthine systems, and negotiating with powerful data brokers—all while managing the immediate risks posed by their abusers.[18] By defaulting to privacy self-management, the legal system fails to protect the vulnerable and allows brokers to

8. Kadri, *supra* note 2, at 138.

9. *See infra* Section I.A.1; Kadri, *supra* note 2, at 150. *See generally* Ignacio Cofone, *Privacy Standing*, 2022 U. ILL. L. REV. 1367, 1403–07 (outlining how privacy invasions can cause "a distinct set of harms in addition to privacy harms," including reputational, financial, discriminatory, bodily, and autonomy harms); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019) (discussing how networked technologies have facilitated various forms of interpersonal abuse).

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

11. Mara Hvistendahl, *I Tried to Get My Name off People-Search Sites. It Was Nearly Impossible.*, CONSUMER REPS. (Aug. 20, 2020), https://www.consumerreports.org/electronics/personal-information/i-tried-to-get-my-name-off-peoplesearch-sites-it-was-nearly-a0741114794.

12. *Id.*

13. Kadri, *supra* note 2, at 153.

14. *See* Ari Ezra Waldman, *Privacy's Rights Trap*, 117 NW. U. L. REV. ONLINE 88, 90–91 (2022).

15. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–83, 1888–93 (2013).

16. *Id.* at 1880.

17. Ella Corren, *Gaining or Losing Control? An Empirical Study on the Real Use of Data Control Right and Policy Implications*, 109 IOWA L. REV. 2017 (2024); *see also* Solove, *supra* note 15, at 1883–93; Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551, 564–67 (2023).

18. *See infra* Part I.

profit from the commodification of personal information.[19] In cases of brokered abuse, obscurity is not a luxury—it is a necessity for survival. The failure of privacy self-management to deliver this obscurity underscores the urgent need for systemic reform.

A fundamental shift in privacy law is needed to center victims and redistribute the burden of achieving obscurity. As Ella's story demonstrates, victims can already be overwhelmed by the challenges of escaping and surviving abuse. The law must instead shift the responsibility for achieving obscurity to the parties who create and profit from the risk: data brokers. These entities possess the resources, technology, and expertise to manage the logistical and technical challenges of obscuring sensitive information. Unlike victims, brokers are well positioned to systematically remove identifying data from their systems and prevent its reappearance. Redistributing this burden would not only be fair but also represent a more effective and sustainable solution to the problem of brokered abuse. By compelling brokers to take responsibility for the risks they create, the law can begin to rectify the systemic injustices that leave victims like Ella fighting for their safety alone.

Redistributing this burden requires a centralized regulatory and technical solution. A fragmented, decentralized approach has proven incapable of addressing the pervasive and evolving threats posed by the broker industry.[20] Victims should be able to invoke their right to obscurity with a single request and expect brokers to honor an ongoing responsibility to identify and remove all relevant information across their databases to ensure no identifying information resurfaces.

This idea has already entered the regulatory imagination, at least in part. California recently passed the DELETE Act,[21] while a federal DELETE Act has also been proposed in Congress.[22] These efforts reflect a small but growing consensus that individuals should not have to navigate hundreds of opaque data broker opt-out processes on their own. Yet these laws suffer from two fundamental flaws. First, they broadly regulate *everyone's* data without tailoring protection to those most at risk, opening them up to viable First Amendment challenges.[23] Scholars like Robert Post, Frederick Schauer, and Amanda Shanor have documented how companies are increasingly wielding the First Amendment to serve a deregulatory agenda,[24] and data brokers have left little mystery as to their willingness to challenge privacy regulations on First Amendment grounds.[25] Accordingly, policymakers should expect fierce First Amendment opposition to privacy regulation and proactively address constitutional scrutiny. Second, the California and federal statutes delegate core technical questions of implementation to future rulemaking,[26] leaving open the risk of ineffective or even injurious compliance mechanisms that entrench broker

19. *See* Woodrow Hartzog, *What is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677, 1683 (2021) (lamenting that few privacy laws "are aimed at disrupting power disparities between people and companies" or "protecting individuals from harassment")

20. *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014); *see also infra* Section I.A.1.

21. S.B. 362, 2023 Leg., Reg. Sess. (Ca. 2023) (California's DELETE Act); *see also infra* Part III.A.

22. H.R. 4311, 108th Cong. § 2(b) (2023); *see also infra* Section III.A.

23. *See infra* Parts III.A.4 & IV.

24. *See* Frederick Schauer, *The Politics and Incentives of First Amendment Coverage*, 56 WM. & MARY L. REV. 1613, 1617 (2015); Amanda Shanor, *First Amendment Coverage*, 93 N.Y.U. L. REV. 318, 322 (2018); Robert Post & Amanda Shanor, *Adam Smith's First Amendment*, 128 HARV. L. REV. F. 165, 166–67 (2015) ("[A]cross the country, plaintiffs are using the First Amendment to challenge commercial regulations, in matters ranging from public health to data privacy.").

25. Letter from Philip Recht, Partner, Mayer Brown LLP, to Senator Kesha Ram Hinsdale, Vt. State Senator 4–7 (Apr. 4, 2024).

26. *See* CAL. CIV. CODE § 1798.99.86; H.R. 4311, 108th Cong. § (2)(a)(1)(A) (2023).

control rather than alleviate the burden on victims. In contrast, this Article offers a detailed regulatory approach that would strengthen both the legal durability and practical efficacy of broker regulation.

To develop and justify our central proposal, this Article builds on scholarship framing obscurity as a discrete privacy interest,[27] highlighting the unique vulnerabilities of abuse victims,[28] critiquing the framework of privacy self-management,[29] and confronting the First Amendment's "Lochnerian" turn.[30] In so doing, this Article makes three main contributions. First, it demonstrates how the combination of decentralized broker opt-out systems and privacy self-management subjects victims to harms beyond those arising from the abuse itself: arduous and relentless vigilance to maintain their obscurity, retraumatization from repeatedly revisiting their abuse, and withdrawal from society for fear of generating more identifying data.[31]

Second, the Article proposes a novel regulatory framework that centers victims and harnesses obscurity to protect human safety. By blending theory, policy, and technical design, the Article presents and justifies a centralized system that would transfer the burden of obscurity onto the billion-dollar industry profiting from brokered abuse.[32] While lawmakers have begun flirting with this idea, the devil is in the details, and this Article answers complex questions about how regulators could implement such an approach—and why they should.[33]

Third, this Article tackles a doctrinal question avoided by many privacy and First Amendment scholars (and by many privacy laws): Can a data-privacy law that covers information gathered from government records and other public sources be constitutional?[34] Through a trio of arguments, the Article confronts the brokers industry's claim that the Constitution insulates them from a centralized obscurity system mandated by law. As an initial matter, the Article challenges the assumption that broker practices are covered by the First Amendment, building on emerging scholarship that questions whether the commodification of personal information serves First Amendment values.[35] It then contests arguments that data dossiers constitute non-commercial speech.[36] Finally, it details why legislating a centralized obscurity system for victims should survive strict scrutiny.[37]

---

27. *See, e.g.*, Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* ROUTLEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY (Joseph Pitt & Ashley Shew eds., 2014); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385 (2013); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013).

28. *See, e.g.*, Thomas E. Kadri, *Networks of Empathy*, 2020 UTAH L. REV. 1075; Kadri, *supra* note 2; Janet X. Chenet al., *Trauma-Informed Computing: Towards Safer Technology Experiences for All*, PROCEEDINGS OF THE 2022 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI '22) 1 (2022); Diana Freed et al., *"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology*, ASS'N COMPUTING MACH. (2018)

29. *See, e.g.*, Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 444 (2016); Solove, *supra* note 15, at 1882–83.

30. Genevieve *Lakier*, *The First Amendment's Real* Lochner *Problem*, 87 U. CHI. L. REV. 1241, 1241 (2020); *see also* Evelyn Douek & Genevieve Lakier, *Lochner.com?*, 138 HARV. L. REV. 100, 103 (2024); Amanda Shanor, *The New* Lochner, 2016 WIS. L. REV. 133.

31. *See infra* Part I.A.2.

32. *See infra* Part II.

33. *See infra* Parts II, III.B–C.

34. *See generally* Thomas E. Kadri, *Platforms as Blackacres*, 68 UCLA L. REV. 1184, 1222–49 (2022) (discussing First Amendment doctrine governing information that has entered the public sphere); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1200–17 (2002).

35. *See infra* Part IV.A.

36. *See infra* Part IV.B.

37. *See infra* Part IV.C.

In doing so, it joins the work of scholars critiquing how expansive interpretations of the First Amendment undermine regulatory efforts and privilege corporate interests over human dignity.

The Article proceeds in four parts. Part I outlines the mechanics of brokered abuse, detailing the inner workings of the broker industry and why its practices endanger victims. It argues that the harms of brokered abuse are not inevitable; rather, they are the result of a broken system that asks too much of the most vulnerable.

Part II then explains why a victim-centered solution demands a paradigm shift in privacy law—one that redistributes responsibility from individuals to the data brokers who profit from their exposure. This Part justifies such a redistribution by emphasizing principles of fairness and efficiency, arguing that brokers, as the least-cost avoiders, are uniquely equipped to shoulder the logistical and technical obligations of obscurity.[38] It concludes by drawing lessons from the private and public sectors to demonstrate the feasibility and efficacy of a centralized approach to obscurity.[39]

Part III provides the statutory and technical blueprint for a centralized system that would allow people like Ella to obscure their information with a single request. It begins by identifying critical gaps in the California and federal DELETE Acts that undermine their ability to deliver meaningful protection.[40] It then presents a detailed framework that integrates a centralized victim opt-out registry, rigorous compliance obligations, and advanced technical tools like cryptographic matching to ensure robust enforcement.[41]

Finally, Part IV confronts thorny First Amendment questions that such a regulatory regime would face. It casts doubt on brokers' claims that a law like this would even trigger constitutional scrutiny before mounting an argument that, at most, our intervention should be assessed under the intermediate scrutiny reserved for regulations of commercial speech. Regardless, this Part concludes by demonstrating why a centralized obscurity system for abuse victims would survive strict scrutiny as a narrowly tailored regulation to achieve a compelling government interest. This doctrinal analysis not only fortifies the proposal against constitutional attack but also contributes to broader debates on the role of the First Amendment in data-privacy regulation.[42]

The status quo requires victims like Ella to manage their own privacy, placing the burden of maintaining obscurity on already-overburdened shoulders. This Article offers a path forward that transforms obscurity from an unobtainable ideal into an enforceable reality.

I. EXISTING LAW AND TECHNOLOGY PUTS THE OBSCURITY BURDEN ON VICTIMS

> *"I was spending hundreds of hours online just looking and searching and going through everything. It's like playing whack-a-mole . . . and it's frustrating because it's such a huge waste of time as well — such a burden on your daily life."* — Ella

38. *See id.*
39. *See infra* Parts II.A.4 & II.A.5.
40. *See infra* Parts III.A.1–A.4.
41. *See infra* Part III.C.
42. *See infra* Part IV.

The responsibility of achieving personal safety through obscurity[43]—or the privacy principle of protecting personal information by making it difficult to access—currently rests almost entirely on the shoulders of victims of abuse. For these individuals, obscurity is not a theoretical concept; it is their best, and often their only, defense against abusers who exploit the data-broker ecosystem to locate, surveil, and harm them.

Yet despite the sometimes life-or-death stakes, victims are expected to navigate a fragmented and convoluted system of opt-out processes to secure this obscurity,[44] shouldering the dual burden of primary and secondary harms. Primary harms arise directly from the loss of obscurity—the stalking, harassment, and violence enabled by data brokers who make sensitive personal information easily accessible to abusers.[45] Secondary harms, by contrast, are inflicted by the privacy system itself, which forces victims to undertake the grueling and often futile task of "privacy self-management."[46]

This dual burden—the risk of exposure on one hand and the impossible demands of self-management on the other—defines the plight of victims in the brokered data economy. These burdens are not merely onerous; they are devoid of empathy.[47] This regulatory failure is a systemic injustice that prioritizes corporate convenience over human safety. It is complicit with the harm perpetrated by abusers and data brokers.[48]

The following section examines these intertwined harms in detail and critiques current privacy laws for their failure to prioritize the safety and dignity of victims.

A. The Harms of Brokered Abuse

The primary harms of brokered abuse—the stalking, the harassment, the physical and psychological threats—are exacerbated by these secondary harms of privacy self-management. The system designed to protect privacy is, for victims, a system that instead inflicts further injury. Obscurity is critical to their safety but achieving it has become tantamount to fighting a broker hydra equipped with little more than desperate conviction.

1. The Primary Harms of Data Exposure

For victims of abuse, obscurity is not an abstract privacy ideal; it is their best, and often only, defense against abusers.[49] The primary harms of brokered abuse are rooted in the destruction of obscurity.[50] By making sensitive personal information easily accessible, data

43. This Article focuses on the concept of obscurity within broader privacy law discourse. Obscurity offers victims a more expansive and operational remedy to the harms of data broker-enabled surveillance. *See generally* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385 (2013); Hartzog & Evan, *supra* note 7; Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way to Think About Your Data Than 'Privacy*,*'* ATLANTIC (Jan. 17, 2013).

44. *See generally* Waldman, *supra* note 14; Solove, *supra* note 15, at 1880.

45. *See* Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1042, 1049–55 (2018); Cofone, *supra*,note 9, at 1367; Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 830–61 (2022). *See also* Scott Skinner-Thompson, *Agonistic Privacy & Equitable Democracy*, 131 YALE L.J.F. 454, 456 (2021).

46. Solove, *supra* note 15, at 1881; *see also* Danielle Keats Citron, *Spying Inc.*, 72 WASH. & LEE L. REV. 1243 (2015).

47. *See* Kadri, *supra* note 28, at 1078–80, 1118–19 (arguing that empathy should be a guiding principle in regulating tech-enabled abuse).

48. Frank Pasquale, Opinion, *The Dark Market for Personal Data*, N.Y. TIMES (Oct. 16, 2014), https://www.nytimes.com/2014/10/17/opinion/the-dark-market-for-personal-data.html.

49. *See* Kadri, *supra* note 2, at 142.

50. Kadri, *supra* note 2, at 138.

brokers empower abusers to locate and target their victims.[51] Commodifying obscurity can manifest physical, psychological, financial, and social harms for those who are vulnerable or in life-threatening situations.

The data broker industry represents a sprawling, multibillion-dollar ecosystem that harvests and sells personal information.[52] There is little oversight or accountability.[53] These companies build their businesses by acquiring and repackaging information from both public records and private sources, often without explicit permission from the people whose lives they catalog.[54] At a minimum, brokers aggregate public documents, accessible to anyone with the wherewithal to request them, such as property deeds, voter rolls, and marriage licenses.[55] Many weaponize transparency tools, such as the Freedom of Information Act (FOIA) to obtain government held personal information[56] and partner with third parties to collect data about online behaviors from apps, ecommerce, social media, and subscription services.[57] Advanced technologies, such as facial recognition and real-time geolocation tracking, supercharge datasets with unprecedented accuracy and granularity.[58] The proliferation of machine learning models enables brokers to infer new data points—including religion, sexual orientation, or even mental health—from existing datasets.[59] These curated dossiers form the core of the broker business model.[60] While there are arguable benefits to data brokerage—such as its use in journalism,[61] law enforcement,[62] and reconnecting with lost relatives[63]—the potential for harm is both pervasive and severe.[64]

---

51. Kadri, *supra* note 2, at 150.

52. *See* Salome Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 588 n.19 (2021). For important early scholarship on brokers, see Hoofnagle, *supra* note 6; Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357. For more contemporary reporting, see Adi Robertson, *The Long, Weird History of Companies That Put Your Life Online*, VERGE (Mar. 21, 2017), https://perma.cc/Z9J8-HU9G; Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, VICE (Mar. 27, 2018).

53. Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, BRENNAN CTR. FOR JUST. (Feb 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.

54. *See* Justin Sherman, *People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs*, LAWFARE (Oct. 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs; *see also* Ashley Kuempel, *The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry*, 36 NORTHWESTERN J. INT'L L. & BUS., 207, 210 (2016).

55. *See* Sherman, *supra* note 54.

56. *See* Kwoka, *supra* note 4, at 125.

57. Ayoub & Goitein, *supra* note 53.

58. *See* Amanda Levendowski, *Resisting Face Surveillance with Copyright Law*, 100 N.C. L. REV. 1015, 1018, 1022–35 (2022); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1485 (2019); Woodrow Hartzog & Evan Selinger, *Why You Can No Longer Get Lost in the Crowd*, N.Y. TIMES (Apr. 17, 2019).

59. *See* Justin Sherman, *How Shady Companies Guess Your Religion, Sexual Orientation, and Mental Health*, SLATE (Apr. 26, 2023), https://slate.com/technology/2023/04/data-broker-inference-privacy-legislation.html. *See generally* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357 (2022).

60. Ayoub & Gotein, *supra* note 53.

61. *See* Thomas E. Kadri, *supra*, note 34, at 1184–87; Thomas E. Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. 951, 977–82 (2021).

62. *See* Andrew Wade, Note, *The Clocks are Striking Thirteen: Congress, Not Courts, Must Save Us From Government Surveillance Via Data Brokers*, 102 TX. L. REV. 1099, 1106 (2024).

63. *See* DELETEME, https://joindeleteme.com/what-are-data-brokers.

64. Urbano Reviglio, *The Untamed and Discreet Role of Data Brokers in Surveillance Capitalism: A Transnational and Interdisciplinary Overview,* 11 INTERNET POL'Y REV., no. 1, 2022, at 1, 15. https://policyreview.info/articles/analysis/untamed-and-discreet-role-data-brokers-surveillance-capitalism-transnational-and. (Figure illustrating 8 different risks of data brokers being under-regulated).

At the forefront of these harms is the erosion of obscurity, perpetrated by the abusers exploiting brokered data and the data brokers who let them.[65] The broker ecosystem arms malicious actors with the ability to reconstruct a target's personal history, locate their current whereabouts, or predict their movements.[66] Through these services, abusers can gain access to otherwise be difficult or impossible to acquire information. For example, a victim may relocate, change phone numbers, enroll in address confidentiality programs, and take other steps to disappear in vain when a broker sells their updated information.

Worse still, brokers make these weaponizable dossiers cheaper and easier to access than ever,[67] paving the way for nefarious use.[68] Tracking someone once required significant financial and logistical effort—hiring private investigators, obtaining court orders, or waiting for public records to update. Today, abusers can purchase detailed reports on a victim's location, family connections, and employment history for as little as a few dollars.[69] This democratization of surveillance tools transforms victims' lives into open books, indexed for convenience, and accessible to anyone with a computer, an internet connection, and a credit card. In this way, brokers render even the most robust of protective measures futile.[70]

The pervasive and persistent availability of brokered data undermines victims' ability to rebuild their lives, forcing them into cycles of isolation and hypervigilance. Obscurity is not just about safety—it is a prerequisite for healing and stability.[71] Without it, victims live in constant fear of discovery, unable to feel secure in their surroundings or relationships. Advanced tools turn fleeting interactions into lasting vulnerabilities and loved ones into unwitting accomplices to abuse. For example, facial recognition databases can turn a single photo uploaded to social media by a friend into a surveillance data point. Similarly, the decision to kill time on Candy Crush[72] can generate real time location data for the taking. Even attempts to adopt new routines could be thwarted by behavior modeling tools that allow abusers to anticipate a victim's actions or locations based on historical patterns.[73]

The erosion of obscurity forces victims to withdraw from social and professional life to avoid leaving traces that could expose them to harm. Fear of exposure can lead victims to delete social media accounts, avoid professional networking, decline opportunities that might publicly associate them with a new location, and even refrain from voting.[74] While these steps may reduce immediate risk, they come at a steep cost, cutting victims off from the support systems and opportunities necessary to rebuild their lives.[75] This isolation not only deepens the psychological wounds inflicted by abuse but also amplifies the societal

---

65. *See* Selinger & Hartzog, *supra* note 27, at 119.

66. *See, e.g.*, *The Amy Boyer Case*, ELEC. PRIV. INFO. CTR. (June 15, 2006), https://archive.epic.org/privacy/boyer; Sherman, *supra* note 54.

67. *See generally* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1995).

68. *See* Citron, *supra* note 9.

69. *See, e.g.*, Sherman, *supra* note 54.

70 Hoofnagle, *supra* note 52, at 595.

71. *See* Chen et al., *supra* note 28, at 1.

72. Joseph Cox, *Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location*, WIRED (Jan. 9, 2025), https://www.wired.com/story/gravy-location-data-app-leak-rtb.

73. *See* Justin Sherman, *Credit Reporting Agencies Don't Just Report Credit Scores*, DUKE SANFORD SCH. OF PUB. POL'Y 9 (Nov. 9, 2022), https://techpolicy.sanford.duke.edu/blogroll/credit-reporting-agencies-dont-just-report-credit-scores.

74. *See* Scottie Andrew, *For Abuse Victims, Registering to Vote Brings a Dangerous Tradeoff*, CNN (Oct. 27, 2020, 3:57 PM), https://www.cnn.com/2020/10/27/us/domestic-violence-voting-election-privacy-trnd/index.html

75. Nicole Froio, *Should Abuse Survivors Have to Disappear from the Internet*, VERGE (Dec. 6, 2021), https://www.theverge.com/22812890/domestic-abuse-survivors-online-presence-spyware-recommendations.

stigma that can accompany such experiences, leaving victims feeling abandoned and unsupported.[76]

The economic impact of losing access to opportunities and resources exacerbates the damage inflicted by brokered abuse. Victims often face significant financial costs associated with escaping abuse, including relocation expenses, legal fees, and lost wages.[77] Forgoing opportunities to earn income or receive external help can make these costs insurmountable. For marginalized individuals, these economic challenges are even more pronounced, as systemic inequities compound the difficulties of navigating both abuse and the exploitative practices of data brokers.[78]

2. The Secondary Harms of Privacy Self-Management

The secondary harms of brokered abuse arise from the expectation that victims are wholly responsible for managing their own privacy to achieve safety—a framework referred to as "privacy self-management."[79] This approach, rooted in the belief that individuals should control how their personal data is collected, shared, and accessed, assumes that individuals are best positioned to make decisions about their privacy and can protect themselves by asserting their rights.[80] However, in practice, particularly in the context of brokered abuse, self-management places an overwhelming and unfair burden on the very people least equipped to bear it.[81] The cumulative toll of this dynamic is profound, encompassing logistical, psychological, and financial costs that victimize individuals anew.[82]

Privacy self-management demands that individuals navigate a convoluted system of data brokers, each with unique and burdensome opt-out procedures.[83] First, victims must scour the internet to identify the brokers that hold their personal information.[84] Then, victims must contact each broker individually to request removal of their data.[85] This often involves submitting detailed forms, verifying their identity, and in many cases, providing sensitive personal documentation, such as copies of government-issued IDs or proof of address.[86] Ironically, the opt-out processes can force victims to hand brokers more sensitive information than brokers had in the first place.[87]

---

76. *See* Kadri, *supra* note 2, at 151.
77. *See id.* at 143.
78. *See* Hvistendahl, *supra* note 11.
79. Solove, *supra* note 18, at 1880–83; *see also* Waldman, *supra* note 14, at 89–90; Kadri, *supra* note 2, at 151.
80. *See* Solove, *supra* note 18, at 1880–83.
81. *See* Corren, *supra* note 17, at 564–67; Solove, *supra* note 18, at 1888.
82. Kadri, *supra* note 2, at 143; Solove, *supra* note 18, at1880–81.
83. *See* Solove, *supra* note 18, at 1888.
84. Hvistendahl, *supra* note 11("No two of these convoluted procedures seem to be alike. People who track the problem estimate that it can take from six business days to two weeks of full-time work to delete your data from data brokers' sites.").
85. *Id.* ("Some sites asked me to enter a current phone number or email address to remove my data, which felt like extortion. Others asked me to register and create a password to "control" my information, without giving me the option to delete it entirely. A few even required me to pick up the phone, send snail mail, or—get this—fax in my request. Where do you even find a fax machine these days?").
86. *See* Kejsi Take et al., *"It Feels Like Whack-a-Mole": User Experiences of Data Removal from People Search Websites*, 3 PROCEEDINGS ON PRIVACY ENHANCING TECH. 159 (2022).
87. *See id.* at 167 ("One [participant] explained that this process can be very difficult for people like themselves who have undergone a name change.").

From a technological perspective, brokers' opt-out systems often lack uniformity or automation, preventing scalable privacy self-management.[88] Some brokers require physically mailed requests, while others mandate the use of proprietary online portals with arcane navigation.[89] Many broker review processes are manual, relying on individual contractors to process opt-out requests. This lack of technical sophistication not only makes the process unpredictable but also ensures that it is both labor-intensive and error-prone.[90]

After all that, there is still no guarantee of obscurity. Even when victims comply with these byzantine requirements, brokers may refuse to act on requests, citing legal exemptions or internal policies.[91] For victims lucky enough to succeed, the same data may resurface[92] or new identifying information may emerge.[93]

For some individuals, third-party services offer a partial reprieve. These services, such as DeleteMe[94] or Privacy Bee[95], act as intermediaries, navigating the complex web of brokers on behalf of their clients. By consolidating the opt-out process, they reduce victims' direct interaction with brokers, allowing them to work through a single point of contact. However, these services come with significant shortcomings.[96] They can be prohibitively expensive[97] and limited in scope, often addressing only high-profile brokers. Additionally, even the best-intentioned services cannot guarantee permanent removal of data because of legal loopholes and poor enforcement.[98]

The demands of privacy self-management force victims into an unrelenting cycle of labor and stress. Victims must monitor the internet, follow up on pending requests, submit new ones, and continually search for additional brokers.[99] These efforts consume significant time, money, and emotional bandwidth—resources many victims lack.[100] Opting out often requires taking time off work, incurring costs such as postage fees, and reliving the trauma of their abuse through repeated interactions with brokers.[101] Forcing victims to become full-time stewards of their own obscurity creates a two-tiered system where only those with the means to pay can access meaningful protection.[102]

This systemic burden is compounded by the inherent power imbalance between individuals and the data broker industry. Brokers operate vast, interconnected networks

88. Hvistendahl, *supra* note 11.

89. *Id.*

90. *See id.* ("I found my information reappearing online, too. Five months after opting out from one data broker, my profile reappeared. When I clicked on my name, the page showed a satellite photo of a house where I had once lived."); Yael Grauer et al., *Evaluating People-Search Site Removal Services*, CONSUMER REPS. 10 (Aug. 8, 2024), https://innovation.consumerreports.org/wp-content/uploads/2024/08/Data-Defense_-Evaluating-People-Search-Site-Removal-Services-.pdf. ("As a whole, people-search removal services are largely ineffective. . . . [W]ithout exception, information about each participant still appeared on some of the people-search sites at the one-week, one-month, and four-month intervals.").

91. *See* Kadri, *supra* note 2, at 153.

92. *See*.

93. *See* Grauer et al., *supra* note 90, at 5; Hvistendahl, *supra* note 11; Take et al., *supra* note 86, at 170.

94. DELETEME https://joindeleteme.com/privacy-protection-plans.

95. PRIVACYBEE, https://privacybee.com/.

96. *See* Grauer et al., *supra* note 90, at 10; Hvistendahl, *supra* note 11.

97. For example, the yearly price for DeleteMe starts at $129 per year. *See* DELETEME *supra* note 94.

98. *See* Hvistendahl, *supra* note 11; Kadri, *supra* note 2, at 153.

99. *See* Grauer et al., *supra* note 90, at 5; Hvistendahl, *supra* note 11.

100. Hvistendahl, *supra* note 11.

101. *See* Kadri, *supra* note 2, at 153.

102. *See* Hvistendahl, *supra* note 11.

that aggregate and sell personal information with minimal oversight or accountability.[103] Victims, by contrast, are left to navigate this labyrinthine system alone, often with no clear guidance or assurance that their efforts will result in meaningful protection.[104] The asymmetry of information, resources, and power ensures that victims are set up to fail, leaving them exposed and disempowered—robbed of agency over their own safety.[105]

The retraumatization caused by engaging with these processes compounds the psychological harm victims endure.[106] Each form submitted, each identity verified, and each explanation of abuse drags victims back into the shadows of their trauma.[107] Some brokers even demand detailed documentation of abuse, such as restraining orders, police reports, or affidavits—forcing victims to reopen old wounds repeatedly for brokers who are neither trauma-informed nor concerned with victim dignity.[108] The very act of putting these experiences into words can be deeply triggering, confronting victims with the fear, pain, and humiliation they understandably hope to leave behind.[109] Further, the demand to hand over personal information can feel eerily reminiscent of the invasions of privacy they experienced at the hands of their abusers.[110]

By leaving victims with no option other than to pursue obscurity through privacy self-management, the law neglects the unique vulnerabilities and lived experiences of brokered abuse victims. This framework prioritizes corporate convenience over human safety, creating systemic barriers that retraumatize and disadvantage victims while failing to provide meaningful or lasting protection. Addressing this injustice requires a paradigm shift away from placing the burden of safety on victims and toward holding brokers accountable for the risks their practices create.

B. The Inadequacy of Existing Laws

The patchwork of privacy laws in the United States[111] fails to adequately address the primary and secondary harms of brokered abuse, often to the point of complicity.[112] These laws either try to curb brokered abuse narrowly and indirectly[113] or they craft interventions that impose new burdens on victims.[114] Together, they amount to a system where victims must shoulder the overwhelming responsibility of managing their own privacy, while abusers and brokers exploit the gaps with impunity.[115]

Laws addressing abuse fall into two categories: those targeting abusers directly—through criminalizing stalking, harassment, or violence—and those aimed at brokers who

---

103. *See* Brittany A. Martin, *The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era*, 105 IOWA L. REV. 865, 867 (2020).

104. *See* Take et al., *supra* note 86.

105. *See id.*

106. *See* Kadri, *supra* note 2, at 153.

107. *See id.*

108. *See* Hvistendahl, *supra* note 11 ("'Everything you do, you have to reshare your story,' she says. Tunon had started her quest hoping to distance herself from a traumatizing situation, but instead she was continually forced to relive it.").

109. *See* Kadri, *supra* note 2, at 153.

110. *See* Hvistendahl, *supra* note 11.

111. *See generally* DANIEL J. SOLOVE, A BRIEF HISTORY OF INFORMATION PRIVACY LAW (2006).

112. *See* Corren, *supra* note 17, at 551.

113. *See generally* Kadri, *supra* note 2, at 142–48.

114. *See* Kadri, *supra* note 2, at 152.

115. *See* Corren, *supra* note 17, at 551.

facilitate abuse, such as through doxing.[116] While vital in theory, both types are deficient in practice. Laws targeting abusers directly require waiting until broker data is used to perpetuate harm. On the other hand, laws targeting broker activities are closer to addressing the root cause of the problem. However, they often rely on scienter requirements, such as proving intent or knowledge of harm, but brokers sell data dossiers at scale, indiscriminately, frustrating case-specific inquiries about mental state.[117] For instance, California's anti-doxing provisions prohibit sharing registered stalking victims' data with intent to incite harm, but brokers evade liability by disclosing data without vetting purchasers.[118] Without scienter requirements, however, these laws risk running afoul of constitutional protections such as the First Amendment.[119]

Anti-abuse laws are impractical for more than just their substance. Their legal processes typically require victims to interact with police, prosecutors, lawyers, or judges, which could deter many from pursuing claims due to fear, financial barriers, or distrust of institutions. Moreover, proceedings are too slow to address the immediate dangers of brokered abuse, and even successful cases fail to address the systemic issue of brokers continually replenishing their data stockpiles. Victims would need to file repeated claims against new brokers, creating an untenable cycle of litigation that does little to disrupt the larger ecosystem.

Transparency laws aim to address harms caused by the broker industry by shedding light on broker practices either to inform regulators (administrative transparency) or empower individuals (popular transparency).[120] For example, Vermont[121] and California[122] require brokers to register with state agencies and disclose information about their data sources and practices, while California's "right to know" laws[123] allow individuals to access data brokers hold about them.[124] More information about the mechanisms of brokered abuse does little to protect victims from it. In addition to being ineffective, these laws can even sap political will from stronger proposals, allowing brokers to hide harmful practices under the veneer of compliance.[125]

Another approach is stemming the tide of personal data at the source. Longstanding laws prohibit deceptive practices, hacking, and unauthorized scraping,[126] while newer laws, such as the California Consumer Privacy Act (CCPA),[127] seek to limit nonconsensual data collection. However, these measures are riddled with loopholes.[128] The CCPA, for example, exempts "publicly available information" and "truthful information that is a matter of public concern," categories encompassing vast troves of brokered data.[129]

---

116. *See, e.g.*, GA. STAT. ANN. § 16-5-90 (criminalizing the offense of "stalking"); CAL. PENAL CODE § 653.2 (criminalizing doxing).

117. *See* Kadri, *supra* note 2, at 142.

118. CAL. GOV. CODE § 6208.1; *see* Kadri, *supra* note 2, at 142–43.

119. *See* Kadri, *supra* note 2, at 142–43.

120. *See, e.g.*, VT. STAT. tit. 9, § 2446; CAL. CIV. CODE § 1798.99.82.

121. *See* VT. STAT. tit. 9, § 2446

122. *See* CAL. CIV. CODE § 1798.99.82

123. CAL. CIV. CODE § 1798.115.

124. *See id*.

125. *See* Waldman, *supra* note 14, at 88 ("And the history of using individual rights to solve structural problems proves how rights crowd out necessary reform.").

126. *See, e.g.*, CAL. PENAL CODE § 502 ("Unauthorized access to computers, computer systems and computer data.")

127. *See* CAL. CIV. CODE §§ 1798.100–.199.100; CAL. CODE REGS. tit. 11, §§ 7000–7304) (collectively, CCPA).

128. *See* CAL. CIV. CODE § 1798.140

129. *See id.*; *see also* Kadri, *supra* note 2, at 146.

Brokers need not resort to illegal practices when a plethora of information is available legally.

Restricting data disclosure is perhaps the most promising approach but remains fraught with challenges. Some regulations, such as tort liability for disclosing sensitive information or bans on selling location data, address the issue indirectly and incompletely.[130] More direct measures, like California's right to opt-out, allow individuals to prevent businesses from selling their data.[131] For abuse victims, California's Safe at Home program provides more robust protections, requiring brokers to conceal registered victims' home addresses and phone numbers for four years.[132] Victims can also seek damages for intentional violations.[133] However, victims must still approach brokers individually, submit forms repeatedly, and monitor compliance over time.[134]

Ultimately, by focusing narrowly on isolated aspects of data brokerage,[135] the existing regulatory responses fail to disrupt the systemic features of brokered abuse.[136] Worse, they impose an untenable burden on victims, making the law complicit in the harm it purports to address.

II. PROTECTING SAFETY THROUGH OBSCURITY DEMANDS REDISTRIBUTING RESPONSIBILITIES

> *"I felt like it was my responsibility to do the opting-out. . . . [I]t was this thought that if I left any kind of stone unturned, that would cause harm to me or my family [. . .] Why should this be a responsibility that I need to bear?"* — Ella

This section contends that addressing brokered abuse requires a paradigm shift in privacy policy that prioritizes meaningful protections for victims while gradually redistributing responsibility to those profiting from their exposure. The consequences of inaction are dire: if we wait for an elusive federal privacy panacea, abusers and data brokers will continue to exploit the gaps in current law, exposing victims to primary harms like stalking and harassment, as well as the retraumatizing secondary harms of navigating a fractured system to protect themselves. Recasting the pursuit of privacy as the pursuit of safety underscores the need for a centralized obscurity system for victims. Drawing on models from the private and public sectors, the section illustrates the feasibility and urgency of holding brokers accountable while relieving victims of unsustainable and unjust burdens.

A. Redistribution of Responsibilities and Ongoing Obligations

To address the systemic failures of brokered abuse and privacy self-management, we must reframe victim privacy as a shared responsibility to promote safety and redistribute

130. *See, e.g.*, *GM Agrees to 5-year Ban on Selling Drivers' Location Data*, REUTERS (Jan. 16, 2025, 6:56 PM) https://www.reuters.com/business/autos-transportation/ftc-bans-gm-disclosing-driver-consumer-data-consumer-reporting-agencies-2025-01-16.

131. CAL. CIV. CODE § 1798.120.

132. *See About Safe at Home*, CAL. SEC'Y STATE, https://perma.cc/4AVJ-TDK3; *see also* Kadri, *supra* note 2, at 148–49.

133. *See About Safe at Home*, *supra* note 132; *see also* Kadri, *supra* note 2, at 148–49.

134. *See* Kadri, *supra* note 2, at 148–49.

135. *See* Kadri, *supra* note 2, at 153.

136. *See* Solove & Hoofnagle, *supra* note 72, at 367 ("In sum, the database industry is increasingly straining the regulatory regime for information privacy established in the early 1970s.").

the labor of achieving obscurity from victims to data brokers. This section argues that a safety-focused approach to obscurity also demands the imposition of ongoing broker obligations to keep victim data offline as well as a centralized governance and enforcement mechanism.

1. Justifying Redistribution

Privacy self-management is nothing short of a systemic failure, an indefensible abdication of responsibility by policymakers.[137] This framework is ill-suited for the average individual, let alone for the most vulnerable among us—people fleeing violence, harassment, and exploitation.[138] A safety-focused lens for obscurity demands a paradigm shift.

The concept of privacy self-management assumes that victims can and should be responsible for navigating a minefield of data brokers, each with their own processes, policies, and pitfalls.[139] It demands vigilance, technical sophistication, and access to time and resources that is rare even among the most privileged.[140] For victims of abuse, this model is not just burdensome; it is retraumatizing.[141] By requiring victims to continually interact with a system that exposed them in the first place, we force them to confront their trauma repeatedly, compounding psychological harm.[142] Victims will always need to play some role in their own protection; asserting the right to obscurity is a necessary initial step. However, this invocation of their right to obscurity should mark the end—not the beginning—of their involvement.

Principles of fairness and efficiency support this reallocation of responsibility. From a fairness perspective, data brokers are the most appropriate entities to bear this burden. These brokers profit directly from the dissemination of data dossiers that disproportionately harm vulnerable populations. Holding brokers accountable for brokered abuse aligns with societal norms that require industries to mitigate the risks they create, much like environmental regulations compel polluters to bear cleanup costs.[143]

Moreover, brokers are the least-cost avoiders—the entities best positioned to implement systemic solutions. With centralized databases, established processes for managing data, and advanced technological capabilities, brokers can integrate obscurity protections far more efficiently than individual victims.[144] The cost of such measures would be modest for an industry already thriving on the commodification of personal data, while the cost to victims of managing their own obscurity is immense. For victims, this redistribution is a lifeline; for brokers, it is a manageable adjustment.

1. Ongoing Duties

Obscurity calls for more than a one-time response to an opt-out request. Redistributing responsibility to brokers must also include ongoing obligations to keep victim information perpetually offline. The reality of data brokerage is that information flows constantly

---

137. *See* Freed et al., *supra* note 28; Kadri, *supra* note 2, at 154.
138. *See* Kadri, *supra* note 2, at 154.
139. *See* Solove, *supra* note 18, at 1881; Corren, *supra* note 17, at 551; Take et al., *supra* note 86.
140. *See* Take et al., *supra* note 145.
141. *See* Kadri, *supra* note 2, at 152–54.
142. *See id.*
143. *See id.*
144. *See id.*

through partnerships, secondary markets, and automated data scrapers.[145] Without robust mechanisms to prevent the re-collection and redistribution of data, any initial removal will be rendered meaningless.[146]

Brokers must implement systems that proactively guard against re-exposure. This includes closing loopholes that allow data to re-enter their networks, monitoring compliance through periodic audits, and collaborating to eliminate weak points in the broader ecosystem.[147] Treating obscurity as a one-time obligation ignores the nature of the threat: victims' safety depends on sustained vigilance.

2. Centralized Governance and Oversight

Even with brokers bearing greater responsibility, effective protection for victims requires centralized governance to coordinate and enforce compliance. Individual brokers cannot be trusted to regulate themselves in a decentralized system riddled with gaps and inconsistencies. [148] A centralized framework, overseen by government regulators, would provide the necessary structure to ensure that brokers fulfill their obligations.

This system would shift the burden of oversight away from victims, who are currently forced to monitor their own exposure and pursue opt-out processes individually. Instead, the government would take on the responsibility of systemic oversight, creating mechanisms for victims to report noncompliance and for regulators to periodically audit brokers. By centralizing these functions, the framework would provide victims with a single point of recourse, relieving them of the impossible task of managing their own privacy across a fragmented landscape.

Centralized governance also ensures accountability at a systemic level, addressing gaps in enforcement that allow brokers to evade meaningful consequences.[149] By integrating oversight into a unified framework, policymakers can create a cohesive system that reinvigorates online obscurity as a meaningful protection for victims while streamlining compliance for brokers.

B. The Case for a Centralized, Coordinated Intervention

A centralized, coordinated system is the most effective way to reallocate the burden of achieving responsibility away from victims and onto data brokers, while ensuring the system has ample oversight. Such a system would enable victims to reclaim their obscurity with a single request, dramatically reducing the overwhelming labor currently required to achieve even temporary relief. Once a request is submitted, brokers—not victims—would bear the responsibility for ensuring that personal information is removed and remains inaccessible into the future. The viability of this approach is well-established, with existing models in both the private and public sectors proving its feasibility and efficacy.

---

145. *See* Rostow, *supra* note 4, at 674.

146. *See* Reviglio, supra note 64, at 12 ("The truth is that once personal information has been packaged, sold and resold, it may live indefinitely in the servers run by the data broker industry.").

147. *See* S.B. 362, 2023 Leg., Reg. Sess. (Ca. 2023) ("Beginning January 1, 2028, and every three years thereafter, a data broker shall undergo an audit by an independent third party to determine compliance with this section.").

148. *See* FED. TRADE COMM'N, *supra* note 20.

149. *See id.*, at ix, 53.

1. Lessons from Private Sector Coordination

The private sector has already demonstrated the effectiveness of centralized coordination in addressing systemic threats, particularly in protecting vulnerable individuals. A compelling example is STOP Non-Consensual Intimate Image Abuse (STOP NCII), a global initiative led by social media platforms that helps individuals prevent the spread of intimate images shared without their consent.[150] This system provides a model for how data brokers could address brokered abuse by creating centralized mechanisms to identify universally harmful information and coordinate efforts to keep it offline.[151]

STOP NCII empowers individuals to leverage the technological capabilities and informational advantages of social media platforms to proactively prevent their intimate images from being shared without consent across participating platforms.[152] Through a centralized system, individuals can submit hash values—unique digital fingerprints—of their intimate images without sharing the images themselves.[153] Platforms such as Facebook, Instagram, and TikTok use this database to identify and block these images before they are distributed, ensuring that victims are not retraumatized by the repeated appearance of harmful content.[154] This approach minimizes the labor required from victims, who otherwise would need to request takedowns across multiple platforms and instead shifts the responsibility onto the platforms to prevent harm.[155]

Policymakers stand to learn a lot from this system as they craft a centralized solution to address brokered abuse. Just as STOP NCII enables victims to take preemptive steps to protect themselves, a centralized obscurity system could allow victims to submit a single request to remove personal information across all covered data brokers. Brokers would then bear the responsibility of ensuring that the flagged data is removed and does not reappear in their networks. Similarly, STOP NCII demonstrates how an empathetic solution must not force victims to share the very information they seek to obscure as a condition to invoking this protection. STOP NCII allows victims to submit hashes of the photos they want to obscure. A system addressing brokered abuse should also only require victims to submit the minimum amount of personal information required by brokers to identify data points to obscure.

STOP NCII also demonstrates the feasibility of centralized coordination in addressing systemic harms. Participating platforms collaborate to maintain a shared database, use existing technologies to enforce compliance, and recognize their shared responsibility to protect vulnerable users.[156] This model proves that a centralized approach is not only operationally viable but also essential for addressing harms that disproportionately affect vulnerable groups.[157] Data brokers could adopt a similar framework, leveraging their extensive technological resources to protect individuals whose personal information exposes them to significant risks.

---

150. *See* STOPNCII.ORG, https://stopncii.org.
151. *See How StopNCII.org Works,* STOPNCII.ORG, https://stopncii.org/how-it-works.
152. *See About Us*, STOPNCII.ORG, https://stopncii.org/about-us.
153. *See How StopNCII.org Works, supra* note 151.
154. *See Industry Partners*, STOPNCII.ORG, https://stopncii.org /partners/industry-partners.
155. *See How StopNCII.org Works, supra* note 151.
156. *Id.*
157. *Id.*

While STOP NCII relies on users to submit hashes for the images they seek to take down, victims of brokered abuse cannot be expected to identify every single piece of information that puts them at risk and requires removal.[158] However, examples from the private sector show that companies can coordinate to identify harmful content even without relying entirely on individual submissions. For example, companies like Pinterest,[159] Instagram,[160] and YouTube[161] collaborate to detect and remove self-harm and suicide-related material.[162] These platforms use centralized tools such as machine learning algorithms to identify patterns, such as flagged keywords, imagery, and behavior, and share insights across platforms to ensure that harmful content removed from one site does not reappear on another.[163] Instead of requiring victims to painstakingly identify every piece of data that endangers them, data brokers could similarly use pooled technological resources to identify and suppress sensitive information that meets established removal criteria for victims.

2. Centralized Systems in the Public Sector

The public sector also provides compelling precedents for centralized frameworks that redistribute responsibility from individuals to entities better equipped to manage systemic risks. These examples underscore the practicality and effectiveness of centralized governance.

The National Center for Missing & Exploited Children (NCMEC) operates a centralized database to combat child sexual abuse material (CSAM), requiring internet companies to report and remove such content proactively.[164] This system alleviates the burden on victims and law enforcement by shifting the responsibility for monitoring and reporting onto the companies that host or distribute harmful materials. Similarly, the Federal Trade Commission's (FTC) Do Not Call Registry allows consumers to register their phone numbers once, placing the onus on telemarketers to ensure compliance with the list.[165] This system transfers the burden of opting out of telemarketing onto the telemarketers, creating a single, enforceable opt-out mechanism consumers can invoke.[166]

Although the General Data Protection Regulation's (GDPR) "right to be forgotten" is a decentralized privilege residents in the European Union can invoke to request the deletion of their personal data from a specific entity, it still offers valuable lessons for a centralized

158. *Id.*

159. *See Suicide, Self-Harm, and Domestic Violence Prevention*, PINTEREST, https://help.pinterest.com/en/article/suicide-and-self-harm-prevention.

160. *See* Adam Mosseri, *Changes We're Making to Do More to Support and Protect the Most Vulnerable People Who Use Instagram*, INSTAGRAM: OFFICIAL BLOG, (Feb. 7, 2019), https://about.instagram.com/blog/announcements/supporting-and-protecting-vulnerable-people-on-instagram.

161. *See Suicide, Self Harm, and Eating Disorder Policy,* YOUTUBE HELP CENTER, https://support.google.com/youtube/answer/2802245?hl=en.

162. Kalhan Rosenblatt & Maya Eaglin, *Meta Teams Up with Snap and TikTok to Address Self-Harm Content*, NBC NEWS (Sept. 12, 2024, 12:13 PM), https://www.nbcnews.com/tech/social-media/meta-teams-snap-tiktok-address-self-harm-content-rcna170838.

163. *Suicide Prevention*, META: SAFETY CENTER, https://about.meta.com/actions/safety/topics/wellbeing/suicideprevention.

164. *See Our Impact*, NAT'L CTR. FOR MISSING AND EXPLOITED CHILD., https://www.missingkids.org/ourwork/impact.

165. *See National Do Not Call Registry*, FED. TRADE COMM'N, https://www.donotcall.gov.

166. CHRIS JAY HOOFNAGLE, *Privacy Self Regulation: A Decade of Disappointment*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 1, 1–3 (Jane K. Winn ed., 2006).

obscurity system.[167] Once an individual submits a request to a company, the GDPR mandates that the company delete the individual's data and notify any third parties to whom the data has been disclosed to do the same.[168] This creates a network effect of data deletion. A centralized obscurity system can harness the same benefits by mandating that brokers notify upstream suppliers and downstream customers that they may be illegally disseminating victim information.

3. Proof of Concept

The success of these private and public sector initiatives demonstrates that centralized systems are not only feasible but also essential for addressing systemic harms. Data brokers, as the entities most capable of implementing such systems, are uniquely positioned to manage a centralized obscurity system. With their existing technological infrastructure and data management capabilities, brokers can adapt their operations to comply with standardized requirements for victim obscurity requests. The cost of compliance to brokers would be modest compared to the staggering safety benefits this system would provide to victims.

The private sector's voluntary establishment of initiatives like STOP NCII demonstrates two key points. First, some industries are intrinsically motivated to address harmful content affecting their users, even without a legal mandate.[169] In cases like counterterrorism or suicide prevention, companies have acted out of a combination of ethical obligation and reputational risk.

By contrast, data brokers lack such intrinsic motivation. Their profit model thrives on the mass aggregation, sale, and dissemination of personal information, and they operate with minimal interaction with or visibility to the individuals affected by their practices.[170] Brokers face little reputational risk because their operations are largely opaque to the public, and their incentives are fundamentally misaligned with user safety.[171] Unlike technology platforms that depend on user trust, brokers profit regardless of the consequences their data sales have on individuals. This absence of market-driven incentives makes voluntary coordination among brokers highly unlikely, necessitating regulatory intervention to enforce harm reduction practices.

Second, centralized coordination to mitigate harm has proven to be neither unduly burdensome nor technologically infeasible. The willingness of private companies to shoulder the costs of initiatives like STOP NCII voluntarily demonstrates that implementing such systems is operationally realistic, even for complex, interconnected ecosystems. Public sector initiatives like NCMEC's CSAM database and the Do Not Call Registry demonstrate that policy can require companies to reconfigure their operations to meet legal obligations without sinking their operations.

---

167. Regulation 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, Art. 17 [hereinafter GDPR].

168. GDPR 1, 2.

169. *See, e.g.*, Rosenblatt & Eaglin, *supra* note 162.

170. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS 68 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (defining data brokers and noting consumers' lack of awareness of brokers' existence).

171. *Id.*

III. DESIGNING A CENTRALIZED OBSCURITY SYSTEM

> *"I'm like, 'Why?' — so much unwanted contact and more headaches, more calling companies, more procedures to just go through [. . .] Are you going to have 200 bookmarks of data brokers?"* — Ella

Achieving meaningful protection for victims of brokered abuse requires a centralized, enforceable system designed to ensure their personal information remains inaccessible to those who aim to exploit it. This section critically evaluates existing and proposed state and federal regulations addressing data broker harms, highlighting their gaps and inefficiencies. Building on these insights, it outlines a statutory framework specifically tailored to safeguard victims of brokered abuse. Unlike broad policy prescriptions that neglect practical implementation, this section emphasizes the necessity of aligning regulatory design with operational feasibility and the policy's overarching goals. To that end, it explores the technical architecture of the proposed centralized system, illustrating how it can effectively shift the burden of managing obscurity from victims to data brokers while ensuring robust oversight and accountability.

A. Limitations of Current and Proposed Interventions

The first step toward protecting victims of brokered abuse is to evaluate the progress and limitations of existing and proposed regulatory efforts, such as California's DELETE Act[172] and the proposed federal DELETE Act.[173] These initiatives represent important attempts to streamline data removal processes and recognize the untenable burdens placed on individuals.[174] However, both fall short in critical ways, either due to express provisions, omissions, or uncertainties left to future rulemaking. By examining these gaps, this section lays the groundwork for designing a harmonized, comprehensive statutory framework that truly protects victims.

Ultimately, this section demonstrates that while the DELETE Acts take necessary first steps, they remain incomplete. Understanding their limitations is essential for crafting future regulations that effectively redistribute the burden of achieving obscurity from individuals to data brokers, ensuring that the most vulnerable are no longer left to navigate the data-broker ecosystem alone.

1. Common Features

The California DELETE Act and the proposed federal DELETE Act aim to address the privacy challenges posed by data brokers by creating centralized systems that simplify how individuals manage their personal information.[175] Both bills provide consumers with a streamlined process to request the deletion or cessation of the sale of their personal data, replacing the current fragmented and burdensome approach of contacting multiple data brokers individually. These efforts represent a crucial acknowledgment of the need to reduce logistical barriers to achieving obscurity in a complex and pervasive data ecosystem.

Under both acts, data brokers—defined as entities that collect personal information from third-party sources and sell or license it—are the primary covered entities. This

172. S.B. 362, 2023 Leg., Reg. Sess. (Ca. 2023) (California's DELETE Act).
173. H.R. 4311, 108th Cong. (2023).
174. Ca. S.B. 362; H.R. 4311.
175. H.R. 4311; CAL. CIV. CODE § 1798.99.86 (added by California's DELETE Act).

excludes first-party data collectors who use information solely for their own business purposes, limiting the scope of regulation. In California, the DELETE Act builds on the definitions and obligations established under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA). Brokers must register annually with the California Privacy Protection Agency (CPPA), which administers the state's centralized deletion portal.[176] Similarly, the federal DELETE Act proposes a nationwide broker registry and centralized opt-out system managed by the FTC.

Both bills share several features aimed at improving consumer privacy and accountability in the data broker industry. They provide a centralized portal for consumers to submit a single request for data deletion or cessation of data sales, shifting some responsibility away from individuals.[177] Additionally, both require brokers to maintain compliance records and undergo audits every three years.[178] Separately, they require the FTC to verify the identity of requesters to guard against fraudulent deletions.[179] These provisions acknowledge the systemic nature of data broker harms and represent a partial shift toward holding brokers accountable.

While these shared features represent progress, their limitations weaken their ability to protect victims of brokered abuse.[180] The broad exceptions—covering legal obligations, fraud prevention, and First Amendment-protected activities—are expansive, giving brokers considerable discretion to deny opt-out requests. Moreover, neither act provides individuals with a private right of action, leaving enforcement entirely to government agencies and restricting victims' ability to seek immediate remedies for noncompliance.

Together, the DELETE Acts demonstrate an important step forward in regulating the data broker industry but fall short of fully addressing the unique and urgent needs of victims of brokered abuse. To truly effect change, future regulations must narrow exceptions, provide victims with actionable remedies, and shift more accountability onto data brokers to ensure meaningful protection.

2. Differences

The California DELETE Act and the proposed federal DELETE Act take different approaches to regulating data brokers, revealing critical strengths and weaknesses when evaluated against the goal of protecting victims of brokered abuse and shifting the responsibility for achieving obscurity from individuals to brokers.

One major difference lies in the treatment of public information. The California DELETE Act explicitly excludes publicly available data—such as property ownership records, voter registration, or court filings—from the scope of personal information that be removed. This excusion, based on definitions established by the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), leaves significant loopholes that undermine protections for victims.[181] By contrast, the proposed federal

176. CAL. CIV. CODE § 1798.99.82(a).

177. CAL. CIV. CODE § 1798.99.86(a)(2), (b)(1); H.R. 4311 §2(b)(1)(A)(ii); H.R. 4311 § 2(b)(1)(B)(i).

178. CAL. CIV. CODE § 1798.99.86(e)(1) (West 2025) (added by California's DELETE Act); H.R. 4311, 108th Cong. § 2(b)(2)(C)(i) (2023).

179. CAL. CIV. CODE § 1798.99.85 (West 2025) (added by California's DELETE Act); H.R. 4311, 108th Cong. § 2(b)(2)(A)(i) (2023).

180. CAL. CIV. CODE § 1798.99.86(c)(2) (West 2025) (added by California's DELETE Act); H.R. 4311, 108th Cong. § 2(b)(2)(A)(ii) (2023); H.R. 4311, 108th Cong. § 2(f)(3)(B) (2023).

181. CAL. CIV. CODE § 1798.140(v)(2).

DELETE Act does not categorically exclude publicly available information, leaving room for future rulemaking by the FTC to include such data within its scope.[182] This difference could make the federal approach significantly more protective, depending on how the FTC defines the boundaries of "covered" data.

For victims of brokered abuse, the exclusion of publicly available information under California law is particularly problematic. Abusers frequently exploit publicly accessible records to locate or stalk victims, leveraging details like addresses, phone numbers, or workplace information.[183] Although California's law provides meaningful safeguards for certain types of personal information, excluding publicly available data allows brokers to continue amplifying sensitive details, putting victims at risk.[184] Closing this loophole is essential for achieving meaningful obscurity and addressing the systemic exploitation of public records by abusers.

A second difference between the two acts is the compliance timeline for data brokers—neither of which adequately protects victims. The California DELETE Act requires brokers to check the registry every 45 days,[185] while the federal DELETE Act mandates a shorter, 31-day compliance period. [186] Although both laws establish ongoing obligations, these timelines are excessively long for individuals in danger, giving abusers ample time to exploit personal information before it is removed. These delays fail to account for the urgency victims face, particularly in situations of imminent threat, and undermine the laws' intent to protect vulnerable individuals quickly and effectively.

From a technological standpoint, such long timelines are unnecessary. Data brokers already operate advanced systems capable of processing vast quantities of information quickly.[187] The centralized registries envisioned by these laws are designed to simplify compliance, meaning brokers could easily process and act on deletion requests within far shorter timeframe—potentially within days, if not hours. By allowing brokers such extended leeway, both laws dilute their effectiveness and maintain the burden on victims to remain vigilant in the interim. Shortening these timelines would not only enhance protections for abuse survivors but would also hold brokers accountable for leveraging their technological capabilities to ensure privacy and safety.

3. Omissions

Both the California DELETE Act and the proposed federal DELETE Act make significant strides in regulating data brokers, but they suffer from critical omissions that undermine their effectiveness, particularly for victims of brokered abuse. Key gaps—such as the lack of a private right of action,[188] the absence of an appeals process for denied requests, [189] and the failure to impose ongoing duties on brokers to ensure deleted data

182. H.R. 4311, 108th Cong. § 2(b)(2)(A)(ii) (2023).
183. Sherman, *supra* note 54.
184. CAL. CIV. CODE § 1798.140(v)(2) (West 2025).
185. *Id.* § 1798.99.86(c)(1)(A).
186. H.R. 4311, 108th Cong. § 2(b)(1)(C)(i) (2023).
187. *See* Kuempel, *supra* note 54, at 219–21.
188. *See* Wade, *supra* note 62, at 1129–30 ("Because the Delete Act lacks a private cause of action, residents cannot hold non-compliant brokers accountable themselves; they must trust that the California Privacy Protection Agency will do it for them—a needlessly risky bet.").
189. *See generally* S.B. 362, 2023 Leg., Reg. Sess. (Ca. 2023); H.R. 4311, 108th Cong. (2023).

remains off their systems[190]—leave individuals with limited protection and perpetuate the burden of achieving obscurity.

One of the most significant omissions is the lack of a private right of action. Both laws delegate enforcement to government agencies—the California Privacy Protection Agency (CPPA) and the California Attorney General for the DELETE Act, and the FTC and potentially state attorneys general for the federal DELETE Act.[191] This setup forces victims to rely on slow and resource-intensive government investigations to address noncompliance, delaying relief for individuals who may face imminent risks.[192] For victims of brokered abuse, whose safety often depends on immediate action, this reliance can result in prolonged exposure to harm.[193] Allowing individuals to directly sue noncompliant brokers would provide an immediate remedy and serve as a stronger deterrent, encouraging brokers to prioritize compliance.[194]

Another critical omission is the lack of an appeals process for denied deletion requests. Both bills allow brokers to deny requests under broad exceptions, such as for legal obligations, fraud prevention, or First Amendment-protected activities.[195] However, neither bill establishes a clear and accessible mechanism for individuals to challenge such denials.[196] Instead, they defer the issue to future rulemaking by the CPPA and FTC, leaving victims with little recourse in the meantime. [197] For victims of brokered abuse, this gap is especially damaging, as it forces them to navigate a system where unjustified denials can leave their sensitive information exposed indefinitely. A robust appeals mechanism—complete with defined timelines and requirements for brokers to justify denials—would ensure individuals have a fair and reliable process to contest decisions, reducing delays and enhancing accountability.

4. First Amendment Vulnerabilities

The California DELETE Act and the proposed federal DELETE Act face substantial First Amendment challenges due to the broad scope of their regulatory frameworks.[198] These vulnerabilities arise from the *combination* of the laws' universal scope, treatment of publicly available information, and selective targeting of data brokers, which *collectively* weaken their ability to withstand constitutional scrutiny.

---

190. *See* Nicole A. Ozer, *Golden State Sword: The History and Future of California's Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age*, 39 BERKELEY TECH. L.J. 963, 1069 (2024).

191. CAL. CIV. CODE § 1798.99.82 (West 2024); H.R. 4311, 108th Cong. § 2(c) (2023); *see also Analysis of the California Delete Act (SB 362) – Signed by Governor Newsom into Law*, TOM KEMP (Oct. 10, 2023), https://www.tomkemp.ai/blog/2023/10/10/analysis-of-the-california-delete-act-sb-362-signed-into-law.

192. *See, e.g.*, Citron & Solove, *supra* note 45, at 822 ("The main benefit of a private right of action in a law is to encourage private enforcement of that law because government agencies often lack the resources to enforce a law rigorously and consistently enough."); *see also See* Ozer, *supra* note 190, at 1071 ("[G]overment enforcers have limited bandwidth and sometimes-conflicting internal interests related to government surveillance and consumer privacy.").

193. *See* Kadri, *supra* note 2, at 152.

194. When CA considered the CCPA in 2018, Attorney General Xavier Becerra wrote to then Assemblymember Ed Chau and Senator Robert Hertzberg emphasizing the need for a private right of action. See Letter from Attorney Gen. Xavier Beccera to Assemblymember Ed Chau and Senator Robert Hertzberg (Aug. 22, 2018). *See also* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1941–46 (2019) (describing advantages of state-law private enforcement remedy for data misuse).

195. H.R. 4311, 108th Cong. § 2(b)(2)(A)(ii) (2023); CAL. CIV. CODE § 1798.99.86 (West 2025).

196. *See* H.R. 4311, 108th Cong. § 2(b)(2)(A)(ii) (2023); CAL. CIV. CODE § 1798.99.86 (West 2025).

197. *Id.* § 1798.99.87.

198. *See* Ozer, *supra* note 190, at 1034–35.

One critical issue is the universal application of both acts to all individuals, regardless of their unique need for protection. While this broad scope is intended to promote consumer privacy, it risks overreach by regulating the dissemination of truthful, at times public, information without distinguishing between individuals facing significant risks—such as victims of brokered abuse—and those with minimal privacy concerns. Courts may find this lack of tailoring problematic under the First Amendment, as the laws could be deemed more speech restrictive than necessary to achieve a compelling governmental interest.[199]

Additionally, both acts selectively target data brokers while excluding other entities that make similar commercial sales of identifiable information, such as social media platforms and e-commerce companies. The statutes narrowly define a "data broker" as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."[200] This definition explicitly excludes platforms like Facebook or Google that collect personal information directly from their users and sell identifiable versions of this information to third parties.[201] While Facebook's activities—selling identifiable user data to entities or individuals—are functionally similar to the practices of data brokers, they fall outside the scope of the DELETE Acts because the company has a direct relationship with its users.[202] This gap highlights a critical limitation of the laws, as it allows entities engaged in significant privacy-compromising activities to evade regulation.[203] The omission is particularly troubling given that these platforms' sale of user data can create the same harms the statutes aim to address, such as enabling harassment, stalking, or other forms of abuse.[204]

This selective targeting raises concerns about underinclusivity, as the laws impose obligations on traditional data brokers while allowing other companies that engage in comparable privacy-compromising behaviors to operate without restriction. Courts have previously scrutinized such regulatory disparities, particularly when they involve the dissemination of truthful information.[205] By failing to cover entities like Facebook that might sell data dossiers, the statutes risk undermining their own objectives and inviting legal challenges.

Together, these issues highlight the DELETE Acts' vulnerability to First Amendment challenges. While their broad application reflects a commitment to consumer privacy, their lack of precision and gaping exceptions expose them to significant legal risks. By contrast, a more narrowly tailored approach—such as the centralized obscurity system proposed in

---

199. *See, e.g.*, NetChoice, LLC v. Bonta, 113 F.4th 1101, 1121 (9th Cir. 2024) (finding provision of the California Age-Appropriate Design Code Act likely to fail strict scrutiny as the State could have "employed less restrictive means to accomplish its protective goals").

200. CAL. CIV. CODE § 1798.99.80 (West 2025); H.R. 4311, 108th Cong. § 2(f)(3)(A) (2023) (excluding entities with direct relationships to individuals whose data they sell from the definition of data broker).

201. *See* AMNESTY INT'L, SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS 10 (2019), https://www.amnesty.org/en/documents/pol30/1404/2019/en.

202. *See* Kurt Knutsson, *How the Delete Act Misses Big Tech Culprits in a Law Designed to Protect Consumers*, FOX NEWS (Oct. 19, 2023, 2:36 PM), https://www.foxnews.com/tech/delete-act-misses-big-tech-culprits-law-designed-protect-consumers ("[T]he concerning culprits of social media companies like Meta's Facebook and Instagram were given a pass and not included in the Delete Act signed into law by Gov. Gavin Newsom.").

203. *See* FED. TRADE COMM'N, A LOOK BEHIND THE SCREENS: EXAMINING THE DATA PRACTICES OF SOCIAL MEDIA AND VIDEO STREAMING SERVICES 37 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.

204. *See* FED. TRADE COMM'N, *supra* note 20.

205. *See, e.g.*, Sorrell v. IMS Health Inc., 564 U.S. 552, 564 (2011); *see also* G.S. Hans, *No Exit: Ten Years of 'Privacy v. Speech' Post-Sorrell*, 65 WASH. U. J. L. & POL'Y 19, 32-37 (2021) (collecting cases considering challenges to privacy laws post-*Sorrell*).

this Article—that closes problematic loopholes can address the harms of brokered abuse more effectively while passing constitutional scrutiny.

B. Regulatory Design

This section proposes a targeted regulatory framework that directly addresses the shortcomings of existing legislative efforts while focusing narrowly on protecting abuse victims. By narrowing the scope and integrating technical feasibility into regulatory design, this approach reduces First Amendment vulnerabilities, redistributes the burden of obscurity from individuals to data brokers, and ensures more effective and enforceable protections.

This section proposes a new federal statutory scheme to address the pernicious harms posed by data brokers and to protect victims of brokered abuse more effectively than existing legislative efforts. While the California DELETE Act and the proposed federal DELETE Act represent meaningful progress, their shortcomings and constitutional vulnerabilities leave victims of brokered abuse insufficiently protected.[206] This proposal builds on their strengths while taking the critical step of tailoring protections to the specific needs of abuse victims, ensuring both legal durability and impact.

The statutory intervention creates a centralized system that requires brokers to take on the technical and logistical burden of complying with victim requests to opt-out of the dissemination of their personal information. At the heart of the system is a central registry maintaining records of individuals who have invoked their opt-out rights. Data brokers must query this database and take immediate, proactive steps to remove or deidentify covered data. This eliminates the fractured, piecemeal nature of existing opt-out mechanisms, replacing them with a single point of coordination and enforcement.

Given the interstate nature of the data broker industry and the reality that victims often cross state lines to escape abusers, a federal framework is essential for comprehensive and uniform protections.[207] Federal legislation avoids jurisdictional gaps and ensures consistency across states, preventing brokers from exploiting discrepancies in state laws. Additionally, tying the framework to existing federal statutes like the Violence Against Women Act and the Safe Connections Act leverages established definitions and enforcement mechanisms, creating a cohesive legal landscape while enhancing support for victims.

This approach would also allow victims to take advantage of the system seamlessly while engaging with other victim protection services, such as changing their address through a state protection program, obtaining a court order, filing a police report, or seeking support from a domestic abuse hotline or shelter. These points of interaction provide practical opportunities to assert their rights under this statute without additional procedural burdens.

However, in the face of federal inaction, states can still adopt similar statutory proposals to protect their constituent victims. By tailoring this model to fit within state-level programs—such as existing Safe at Home initiatives or domestic violence

206. *See supra* Part III.A.

207. *See* Catherine Stupp, *Patchwork of State Privacy Laws Remains After Latest Failed Bid for Federal Law*, WALL ST. J. (Aug. 27, 2024), https://www.wsj.com/articles/patchwork-of-state-privacy-laws-remains-after-latest-failed-bid-for-federal-law-2a1a020d.

protections—states can achieve meaningful reform and establish localized solutions that address the urgent safety needs of their residents.

1. Invoking the Right: Whom & How

Ultimately, the statute endeavors to protect individuals whose safety and wellbeing are directly endangered by data broker dissemination of their personal information. The goal is to craft a narrowly tailored yet inclusive framework that prioritizes the needs of the most vulnerable victims while avoiding unnecessary exclusions. By drawing on established federal protections like the Violence Against Women Act (VAWA)[208] and the Safe Connections Act,[209] and filling gaps through independent definitions, the statute offers both clarity and flexibility to address emerging forms of brokered abuse.

The statute uses federal family law principles to establish a foundation for coverage, reflecting a tradition of protecting vulnerable individuals in intimate or familial relationships while expanding protections to include non-relational abuse. VAWA defines victims as those subjected to physical, sexual, or psychological harm by intimate partners,[210] while the Safe Connections Act focuses on abuse facilitated through technology.[211] These frameworks provide robust definitions and enforcement mechanisms that this statute can leverage.

However, gaps remain. VAWA's focus on intimate partner violence excludes victims abused by family members, coworkers, acquaintances, or strangers,[212] while the Safe Connections Act primarily addresses telecommunications abuse, neglecting broader harms like doxxing, stalking, and identity theft.[213] To address these gaps, the statute should define specific qualifying acts—such as stalking, harassment, or misuse of personal data—that fall outside the purview of existing federal laws. This approach ensures victims in diverse and nontraditional abuse contexts are included. By grounding eligibility in established federal definitions and supplementing them with independently enumerated harms, the statutory intervention can provide both consistency and flexibility.

Once eligibility is defined, the next question is how individuals demonstrate that they qualify for the right to opt out. The statute should adopt self-attestation as the preferred method, whereby victims submit a sworn statement affirming their eligibility without further evidentiary requirements. This approach minimizes barriers to access this protection and empower victims to invoke their rights without requiring documentation that may be difficult, dangerous, or retraumatizing to obtain. Self-attestation has precedent in federal laws such as the Safe Connections Act,[214] and in family law programs in states like New York,[215] demonstrating its feasibility and effectiveness. This method aligns with the statute's goal of avoiding the major bureaucratic and emotional burdens that obtaining documentations places on the shoulders of vulnerable victims.

---

208. Violence Against Women Act of 1994, 42 U.S.C. §§ 13925–4045d.

209. Safe Connections Act of 2022, 47 U.S.C.A. § 345 (West).

210. 42 U.S.C. § 13925.

211. 47 U.S.C.A. §§ 345 (West).

212. *Community Explainer: Who Is Eligible For VAWA?*, IMMIGRANT LEGAL RESOURCE CENTER (Dec. 2022),https://www.ilrc.org/sites/default/files/2023-02/Who%20is%20Eligible%20for%20VAWA%3F.pdf.

213. 47 U.S.C.A. § 345 (West).

214. *Id*.

215. N.Y. Pub. Serv. Law § 48-A (McKinney 2024).

While requiring documentation—such as police reports, protective orders, or affidavits from counselors—might theoretically add a layer of verification, it is not an ideal solution. Victims often face significant hurdles in obtaining these materials,[216] whether due to distrust of law enforcement, safety concerns, or the sheer difficulty of navigating bureaucratic systems while coping with trauma. Imposing documentation requirements would create an inequitable system where only those with the resources and ability to produce proof are protected. Furthermore, documentation requirements disproportionately exclude individuals in emergency situations or those who fear retaliation for seeking help. Meaningful privacy protections for victims of brokered abuse minimizes, not compounds, the labor these individuals must undertake.

Self-attestation does not pose a significant risk of misuse in this context for several reasons. First, an otherwise ineligible individual invoking the right to opt out of data dissemination does not implicate anyone else's legal rights or entitlements, unlike scenarios involving shared property like vehicles, where granting access to one party necessarily deprives the other. Second, non-victims are unlikely to exploit this system at scale because the process still requires submitting a sworn statement attesting to their eligibility, which serves as a deterrent to frivolous claims or insufficiently motivated individuals.

Finally, the system is unlikely to be weaponized by abusers. While it is theoretically possible for an abuser to attempt to invoke the right to hide their own history of abuse from future connections, relational abuse dynamics are rarely clear-cut. Often, both parties in an abusive relationship can be simultaneously victim and perpetrator, as evidenced by mutual restraining orders or court findings that both parties engaged in harmful behavior. Research also shows that individuals who were victims of abuse in the past are statistically more likely to perpetrate abuse in the future,[217] further complicating the binary distinctions of abuser and victim.

These complexities underscore the importance of maintaining low barriers to access. Raising the threshold for eligibility risks disqualifying otherwise eligible victims in edge cases, particularly those who may not fit traditional or clear-cut narratives of abuse. Such a result would be counterproductive to the statute's goal of providing expansive protections to individuals endangered by brokered abuse. In this context, the psychology and dynamics of relational abuse—where roles of victim and abuser may shift or overlap—demand a nuanced approach that errs on the side of accessibility. By allowing self-attestation, the statute ensures that all eligible individuals, including those in complex or nontraditional abuse situations, can invoke their right to safety without unnecessary procedural hurdles.

By adopting a self-attestation model, the statute ensures that the process of invoking the right is accessible to all victims, regardless of their circumstances. If concerns about misuse arise after implementation, they can be addressed through periodic reviews of the system's operations, as is done for other comparable interventions.[218] However, the statute should prioritize removing barriers for victims rather than preemptively creating hurdles based on hypothetical concerns about bad actors. This approach reflects the statute's

---

216. *Calling the Police Shouldn't Be Another Barrier*, DOMESTICSHELTERS.ORG (Nov. 7, 2016), https://www.domesticshelters.org/articles/escaping-violence/calling-the-police-shouldn-t-be-another-barrier.

217. Elizabeth Hartney, *9 Reasons the Cycle of Abuse Continues*, VERYWELL MIND (Jan. 4, 2024), https://www.verywellmind.com/the-cycle-of-sexual-abuse-22460.

218. *See, e.g.*, National Do Not Call Registry, https://www.donotcall.gov (featuring a feedback provision if you still receive unwanted calls).

broader ethos: redistributing the labor of achieving obscurity away from victims and onto the brokers who profit from their data.

2. Covered Brokers & Data

By holding data brokers accountable for the harms of brokered abuse, the statute aims to redistribute the labor of protecting vulnerable individuals from victims to the entities profiting from the collection and sale of personally identifiable data. To achieve this, the statute consciously employs broad definitions of "data broker" and "covered data" to deliver meaningful protection, and imposes carefully crafted compliance obligations.

Under this statute, a data broker is any entity that collects PII and sells or licenses it to third-parties in a non-deidentified form, irrespective of whether the entity has a direct relationship with the individual from whom the data was collected.[219] This definition ensures coverage of platforms like Google, which collect data directly from users but sell it in various formats to third parties.[220] A narrow definition would create dangerous loopholes, allowing entities to avoid accountability by operating under alternative business models or by selling smaller quantities of data.[221] Lessons from analogous efforts to combat child sexual abuse material (CSAM) reinforce the importance of comprehensive coverage. [222] Just as it is crucial to remove CSAM from all distribution channels to prevent resurfacing, the brokered information that undermines victim obscurity must be comprehensively purged from brokered datasets to ensure safety. [223]

The statute's definition of "covered data" takes a similarly expansive approach to include both direct and indirect information. Direct PII encompasses traditional identifiers like names, addresses, phone numbers, emails, and social security numbers, [224] which are the most immediate and obvious targets for removal.[225] However, the statute also covers indirect data that could endanger victims by providing alternative avenues for harm. For example, records related to family members, employment locations, or roommates can enable abusers to locate or target victims indirectly. [226] To address these risks, brokers are required to use clustering techniques to identify and act on indirect data,[227] guided by thresholds and methodologies developed by experts at agencies like the FTC or National Institute of Science and Technology (NIST). This ensures that tangential connections that

---

219. *See also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS 68 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

220. *See* Chris J. Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 628 (2014) (explaining Google's business model of exchanging a free search engine for information); *see also* Alexander Tsesis, *The Right to Be Forgotten and Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 48 WAKE FOREST L. REV. 101, 105 (2014).

221. *See* Samuel W. Buell, *Good Faith and Law Evasion*, 58 UCLA L. REV. 611, 614 (2011) ("Narrow and hard-edged rules of law create space for evasion.").

222. *See* U.S. DEP'T OF JUST., CHILD SEXUAL ABUSE MATERIAL 10 (2023), https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf.

223. *See* Kadri, *supra* note 2, at 149–54.

224. *See* Jules Polonetsky et al., *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 SANTA CLARA L. REV. 596, 605 (2016).

225. *See* Lauren A. Di Lella, Comment, *Accept All Cookies: Opting-in to a Comprehensive Federal Data Privacy Framework and Opting-Out of a Disparate State Regulatory Regime*, 68 VILL. L. REV. 511, 513–14 (2023).

226. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1841–43, 1847 (2011).

227. For a background on data clustering, see generally DATA CLUSTERING: ALGORITHMS AND APPLICATIONS (Charu C. Aggarwal & Chandan K. Reddy eds., 2014).

abusers might exploit are accounted for, aligning with the statute's goal of providing comprehensive protection. [228]

Including indirect data in the statute's scope imposes a minimal burden on third parties, such as family members, whose information may also be removed. Unlike systems that require these individuals to independently request removal, this statute places the responsibility on brokers, streamlining the process and shifting the burden away from victims and their families. **[229]** Given that brokers already use clustering techniques for commercial purposes, [230] such as creating consumer profiles and linking datasets, [231] this requirement is both feasible and ethically justified. The statute simply compels brokers to repurpose their existing tools and expertise toward protecting vulnerable individuals, rather than solely pursuing profit.

Covered data must also include publicly available data to avoid permitting exceptions that undermine the policy's protective goals.[232] While public records like voter registrations or property deeds are not inherently problematic, brokers exacerbate the risks they pose by aggregating and centralizing this information, making it instantly accessible at scale.[233] Information that is technically public, such as voter registration data or property deeds, can be weaponized by abusers to locate or harm victims. The statute's goal of obscurity is not to erase public records but to restore the practical obscurity that previously limited their accessibility to abusers.[234]

3. Adherence to a Standard of Care

The statute imposes rigorous obligations on data brokers to ensure victims of brokered abuse are protected. Key obligations include prohibitions on dissemination, proactive monitoring, supply chain accountability, and robust compliance measures.

As a threshold requirement, covered data brokers must register with the agency tasked with overseeing the statute's implementation. This builds on successful models like those in Vermont[235] and California[236] and provides regulators with critical insights into the broker ecosystem, facilitating enforcement and the potential for future regulation.

Brokers are explicitly prohibited from publishing, selling, or disseminating identifiable data tied to registered victims. Similar to the Do Not Call Registry,[237] this prohibition does not require outright deletion of data but ensures covered data is not disclosed in any identifiable form. Even pseudonymous data, which risks reidentification, is restricted, allowing dissemination only in fully deidentified formats. This ensures victims' sensitive information is robustly protected without unnecessarily hampering brokers' operational needs.

---

228. *See, e.g.*, Sherman, *supra* note 54.

229. *See* Kuempel, *supra* note 54, at 221–23.

230. *See id; see also* Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 1, 9–11 (2002).

231. *See* Kuempel, *supra* note 54, at 219–21.

232. *See* Rostow, *supra* note 4, at 674, 670–72.

233. *See* FED. TRADE COMM'N, *supra* note 20, at 3, 48–49.

234. *See* Hartzog & Stutzman, *supra* note 58, at 5–8.

235. *See* VT. STAT ANN..Tit. 9, § 2446 (2019).

236. *See* CAL. CIV. CODE § 1798.99.82 (2024).

237. NAT'L DO NOT CALL REGISTRY, FED. TRADE COMM'N, https://www.donotcall.gov.

The statute also imposes a continuing obligation on brokers to monitor their systems to prevent reemergence of covered data. Automated processes must compare newly acquired data against records of registered victims, removing any flagged information before further dissemination. These monitoring obligations extend beyond previously deleted data to include new details like updated addresses, phone numbers, or employment information tied to registered victims. This ensures long-term, dynamic protections for victims rather than one-time removals.

In addition to refraining from disseminating non-deidentified victim data, brokers are also required to notify entities in their data supply chain—both those they acquire data from and those they sell data to—when a dataset contains records about a registered victim. Inspired by GDPR principles,[238] this ensures compliance throughout the data ecosystem. For example, if a downstream buyer unknowingly receives sensitive data, the seller must inform them to prevent further circulation. This creates a cascading effect that reduces the risk of victim information persisting in the ecosystem.

To encourage compliance, the statute can include an immunity mechanism for brokers who inadvertently handle protected data but promptly notify the oversight agency upon discovery. By offering a pathway to avoid punitive measures, this provision incentivizes proactive registration and engagement with the central registry as well as self-monitoring while fostering collective accountability among brokers.

Brokers must also maintain an appeals process for disputes over opt-out requests. While the statute allows certain exceptions for lawful obligations, fraud prevention, or protected First Amendment activities, it ensures victims are not unduly burdened. In contested cases, brokers must default to taking down the data, notify the victim of their intent to invoke an exception, and provide an opportunity for the victim to challenge the exception's applicability. Critically, the burden of proof shifts to the broker to justify the exception, reducing the procedural burden on victims.

Finally, brokers are required to self-attest to compliance, make their books and systems available for impromptu inspection by governing agencies, and submit regular compliance reports detailing actions taken to honor opt-out requests, including records of flagged, deleted, or deidentified data. These measures allow agencies such as the FTC or Consumer Financial Protection Bureau (CFPB) to audit broker activities, identify patterns of noncompliance, and enforce penalties where necessary.

4. Implementation

The successful implementation of this statutory regime depends on a robust and well-funded infrastructure, overseen by a competent federal agency capable of managing its many responsibilities. Whether the FTC or the CFPB assumes this role, [239] the agency must

238. *See generally* GDPR, Art. 17.

239. The FTC, as the primary agency protecting consumers from deceptive and unfair business practices, has already brought multiple enforcement actions against data brokers for abusive data practices. *See* Press Release, Fed. Trade Comm'n, FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data (Dec. 3, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data (announcing an action against a data broker to prohibit the sale of sensitive location data); Press Release, Fed. Trade Comm'n, FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and Inmarket (Mar. 4, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket (announcing actions against data brokers for

handle critical tasks such as maintaining central registries, verifying opt-out requests, monitoring broker compliance, and adapting to emerging risks in the data-broker ecosystem. Two central registries are necessary: one for data brokers and another for individuals opting out of data dissemination. The agency must ensure that opt-out requests are legitimate, preventing misuse such as abusers impersonating victims to manipulate the system. Beyond verification, the agency must monitor compliance by requiring brokers to regularly query the registry, auditing their activity logs to detect anomalies, and addressing complaints from victims and brokers reporting non-compliance. Additionally, the agency must invest in ongoing research to refine key processes like hash matching, clustering, and deidentification, ensuring the system evolves alongside advancements in the broker ecosystem.

Given the wide-ranging responsibilities of the implementing agency, substantial funding will be essential. However, relying on congressional appropriations is impractical in the current political climate. To address this challenge, the statute should require brokers to pay tiered registration fees, scaled by their size or the volume of data they handle. These fees would create a sustainable revenue source to support the agency's work, including audits, enforcement, public education campaigns, and grants for domestic violence shelters or legal aid organizations that assist victims. Penalties collected from noncompliant brokers would also supplement this fund, ensuring a steady stream of resources. This funding model, inspired by the Universal Service Fund in telecommunications, demonstrates how a fee-based system can support comprehensive regulatory frameworks without relying on direct congressional appropriations. [240]

The statute's penalty scheme must be uncompromising in its commitment to protect victims and ensure compliance from brokers. Civil penalties should escalate with the frequency and severity of violations, ensuring that repeat offenders face increasingly harsher consequences. These penalties serve as both a deterrent and a preventive measure, reinforcing the statute's commitment to victims. Equally important is the inclusion of a private right of action, which would empower victims to hold brokers directly accountable. A private right of action would allow victims to, at minimum, recover compensation from brokers for the harm they suffer due to the broker's noncompliance. Even if victims are unable to sue for damages, a private right of action would allow victims to seek injunctive relief from noncompliant brokers—an avenue that is faster than waiting for agency action and cheaper than a civil suit for damages.

In cases where a private right of action is not politically or legally feasible, the tort system offers an alternative mechanism for accountability. Brokers who fail to meet their obligations could still be held liable under common law tort doctrines for breaching their duty of care to victims. Whether through statutory penalties, private lawsuits, or common law remedies, the framework must prioritize victim safety and refuse to dilute protections in favor of abstract compromises or political expediency. Ultimately, the stakes—

---

the sale of sensitive location data). Additionally, the CFPB, an agency with a specialized focus on protecting consumers' financial information, recently proposed a rule to protect the public's personal and financial information. *See CFPB Proposes Rule to Stop Data Brokers from Selling Sensitive Personal Data to Scammers, Stalkers, and Spies*, CONSUMER FIN. PROT. BUREAU (Dec. 3, 2024), https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-stop-data-brokers-from-selling-sensitive-personal-data-to-scammers-stalkers-and-spies. Both agencies are well-positioned to oversee a federal statutory scheme protecting personal and sensitive data.

240. However, constitutional challenges to such fee-based regimes may undercut their feasibility moving forward. *See* Consumers' Rsch. v. FCC, 109 F.4th 743 (5th Cir. 2024), *cert. granted*, SHLB Coalition v. Consumers' Rsch., No. 24-422, 2024 WL 4864037 (Nov. 22, 2024).

protecting lives, safety, and well-being—demand an uncompromising commitment to enforcing these protections.

C. Technical Design

This proposed federal statutory scheme provides the foundation for redistributing the burden of achieving obscurity from individuals to brokers, but its success hinges on the technical infrastructure that implements it. Without a reliable and carefully designed system to operationalize these rights and protections, even the best-intentioned law risks regulatory impotence. This section outlines the technical design considerations of a centralized obscurity system predicated upon a federally maintained database and interoperable standards to ensure uniform compliance across a fragmented, sprawling data broker ecosystem. The proposed system aims to avoid the pitfalls of a piecemeal, privacy self-management approach, offering a scalable and resilient centralized pathway to meaningful reform.

1. The Need for a Prescriptive Technical Solution

Allowing brokers to design and implement compliance systems independently would almost certainly lead to inconsistency, inefficiency, and opportunities for bad-faith circumvention. Data brokers operate within a competitive market where incentives to comply rigorously with privacy protections often clash with profit motives.[241] Historically, self-regulation in industries with significant public interest has resulted in systems designed with inefficiencies—intentional or not—that entrench themselves over time.[242] This form of weaponized path dependency occurs when companies intentionally design systems that are cumbersome and opaque to use when forced to comply with new mandates.[243] Once these systems are in place, the architecture ossifies, and companies exploit the narrative that compliance is inherently expensive and burdensome to resist further regulation or roll back the imposed protections entirely.[244]

A striking example is the ongoing failure to mandate true interoperability in health data across electronic health record (EHR) systems. Despite laws like the Health Information Technology for Economic and Clinical Health (HITECH) Act[245] and subsequent interoperability initiatives, the EHR industry has built fragmented systems full of proprietary standards and data silos. This lack of seamless interoperability is not accidental; it is a calculated feature of self-regulation, aimed at maintaining vendor lock-

---

241. Rostow, *supra* note 4, at 670; *Data Brokers*, ELEC. PRIVACY INFO. CTR., https://epic.org/issues/consumer-privacy/data-brokers.

242. *See* Alyssa Wong, *Regulatory Gaps and Democratic Oversight: On AI and Self-Regulation*, UNIV. OF TORONTO (Sept. 21, 2023), https://srinstitute.utoronto.ca/news/tech-self-regulation-democratic-oversight; *see also, e.g.*, *Corporate Self-Regulation Is a Global Crisis*, HUM. RTS. WATCH (Nov. 14, 2017, 10:01 AM), https://www.hrw.org/news/2017/11/14/corporate-self-regulation-global-crisis; Andreja Marusic & Madelynne Grace Wagner, *How Companies Like Yum! Brands Can Improve Compliance Through Self-Regulation*, WORLD BANK BLOGS (Feb. 20, 2018), https://blogs.worldbank.org/en/psd/how-companies-yum-brands-can-improve-compliance-through-self-regulation.

243. *See* Marusic & Wagner, *supra* note 248.

244. DOUGLAS C. MICHAEL, UNIV. OF KY. COLL. OF L., ADMINISTRATIVE CONF. OF THE UU.S. 21 n.81 (1993), https://www.acus.gov/sites/default/files/documents/1994-01%20The%20Use%20of%20Audited%20Self-Regulation%20as%20a%20Regulatory%20Technique.pdf (citing EUGENE BARDACH & ROBERT A. KAGAN, GOING BY THE BOOK: THE PROBLEM OF REGULATORY UNREASONABLENESS 241 (1982)).

245. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-15, 123 Stat. 115 (2009).

in and avoid competition. Similarly, the rollout of the California Consumer Privacy Act[246] (CCPA) saw companies implement patchwork compliance mechanisms that created consumer confusion and created obstacles to exercising rights.[247] These systems were later cited by industry advocates as evidence of compliance being "too complicated" or costly, fueling lobbying efforts to water down subsequent enforcement or legislative expansion.[248]

By learning from these examples, the proposed statutory scheme prioritizes a centralized technical framework to ensure consistency, eliminate inefficiencies, and prevent evasion. A federal framework avoids the pitfalls of industry-designed systems, ensuring that compliance mechanisms are transparent, effective, and resistant to weaponized inefficiency.

2. Central Victim Opt-Out Registry

The centralized database lies at the heart of this system, maintaining records of individuals who have opted out of having their personal information collected, sold, or otherwise distributed by data brokers. The design prioritizes storing only the minimal information necessary to accomplish the policy's goals, balancing functionality with privacy and security. Unlike a comprehensive repository of every data point a victim wishes removed, the database holds just enough information—such as hashed combinations of names, dates of birth, social security numbers, and aliases—to allow brokers to identify and act on relevant records in their own systems. By limiting the scope of stored data, the database minimizes its attractiveness as a target for attackers while still enabling brokers to meet their obligations effectively. The system will also employ prevailing cybersecurity best practices, to further secure information in the database.[249]

3. Data Broker Queries

Data brokers interact with the centralized database via a secure API endpoint, bearing the computational responsibility for matching records to minimize strain on the central system and protect privacy. The challenge lies in allowing brokers to see whether the data they possess matches the data in the central registry without learning the contents of the central registry or sharing with the central registry all of the personal information they possess. API queries can employ advanced cryptographic techniques that would allow brokers to compare the contents of their databases with the content in the central victim registry without exposing the information they possess or accessing information from the

246. CAL. CIV. CODE § 1798.100–.199.100 (West 2023).

247. *New State Privacy Laws Creating Complicated Patchwork of Privacy Obligations*, BLANK ROME (June 7, 2024), https://www.blankrome.com/publications/new-state-privacy-laws-creating-complicated-patchwork-privacy-obligations; Andrew Bluestein, *With CCPA Looming, Publishers Are Confused and Consumers Are Unlikely to Share Their Data*, THE DRUM (Oct. 3, 2019), https://www.thedrum.com/news/2019/10/03/with-ccpa-looming-publishers-are-confused-and-consumers-are-unlikely-share-their.

248. *See* Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of $55 Billion to Get in Compliance*, CNBC (Oct. 5, 2019, 10:15 AM), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html.

249. To enhance security further, all stored identifiers can be cryptographically hashed with a process known as "salting," where each value is combined with a unique random string before hashing. This ensures that even if the database is compromised, the hashed data cannot be reverse-engineered into its original form without the salt, or the unique random string associated with the record. Andrew Hughes, *Encryption vs. Hashing vs. SaltingWhat's the Difference?*, PINGIDENTITY (Dec. 20. 2024), https://www.pingidentity.com/en/resources/blog/post/encryption-vs-hashing-vs-salting.html.

registry they do not already have.[250] Some techniques enable brokers to identify matches without the central victim registry seeing their datasets,[251] while others ensure the database comparisons occur only in encrypted form.[252] These types of methodologies ensure that brokers fulfill their compliance obligations without further compromising victim privacy.

To accommodate the variability in personal data records—such as nicknames, typos, or alternate spellings—the database must support approximate matching techniques.[253] Algorithms like fuzzy hashing[254] and Levenshtein distance[255] allow brokers to identify close matches rather than relying on exact matches, ensuring that compliance is comprehensive without imposing undue burdens on victims to list all possible variations of their data. Importantly, these approximate matching methods are compatible with the advanced cryptographic protocols the database would use to ensure API queries don't further compromise victim privacy. So, brokers can use approximate matching locally with hashed data to identify variations without revealing their full dataset or accessing unrelated records in the central database. This ensures that variability in data formats does not impede compliance while maintaining robust privacy protections.

Each interaction between a broker and the central database is logged, capturing timestamps, query metadata, and the broker's unique identifier. These activity logs create transparency and accountability, enabling the central database to monitor compliance. Alongside these logs, brokers must also submit compliance reports detailing queries conducted, matches identified, and actions taken, such as records deleted or deidentified. These broker-generated compliance reports allow the central database to audit broker activities and identify discrepancies or patterns of noncompliance to reinforce the integrity of the framework and the protection of victims' data.

To streamline updates, the central database can offer webhook integration. Brokers can subscribe to receive notifications when a registered victim updates or expands their covered data. These notifications would not disclose sensitive information but instead include a broker-specific reference ID and a directive to re-query the database. This approach fosters efficient compliance without exposing unrelated victim data.

4. Identifying Covered Victim Data

Brokers, upon receiving hashed identifiers for individuals who have opted out, must use these hashes to locate and remove or deidentify records containing direct PII such as

---

250. Advanced cryptographic methods such as Private Set Intersection (PSI), homomorphic encryption, and Bloom filters ensure privacy-preserving queries. In these processes, the database and brokers compare hashed identifiers without revealing any additional data that the broker did not already possess. *See generally* Mike Rosulek, *A Brief Overview of Private Set Intersection*, COMPUT. SEC. RES. CTR. (Apr. 19, 2021), https://csrc.nist.gov/presentations/2021/stppa2-psi; *What Is Homomorphic Encryption?*, IBM, https://www.ibm.com/think/topics/homomorphic-encryption; Tristan Garwood, *Saving Money and Protecting Privacy With Bloom Filters*, LOCALYTICS (Aug. 27, 2018), https://eng.localytics.com/saving-money-protecting-privacy-with-bloom-filters.

251. Ulf Mattsson, *Privacy-Preserving Analytics and Secure Multiparty Computation*, ISACA (Mar. 17, 2021), https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/privacy-preserving-analytics-and-secure-multiparty-computation.

252. *What Is Homographic Encryption?*, SUPERMICR, https://www.supermicro.com/en/glossary/homomorphic-encryption.

253. *See generally* Madhurima Nath, *Fuzzy Matching Algorithms*, MEDIUM (Jan. 8, 2024), https://medium.com/@m.nath/fuzzy-matching-algorithms-81914b1bc498.

254. *See* Nath, *supra* note 196.

255. *See generally Levenshtein Distance*, SCI. DIRECT, https://www.sciencedirect.com/topics/computer-science/levenshtein-distance.

social security numbers, names, email addresses, and dates of birth. Often, the ability to pinpoint an individual arises from a combination of elements—like a name paired with a date of birth or an email address tied to a social security number.[256] Using the provided hashed values, brokers must deploy automated matching algorithms to accurately locate and expunge these direct identifiers, ensuring victims' key identity markers are no longer accessible within their systems.

However, obscurity cannot be achieved by removing direct PII alone. In the context of brokered abuse, abusers are often intimately familiar with their victims and can therefore exploit otherwise vague or innocuous data to harm them.[257] To provide meaningful victim obscurity, brokers must also identify and address indirect data points that, while not explicitly identifying an individual, could still expose them to harm.[258] Indirect data might include records tied to family members, roommates, or frequent contacts—information that an abuser could exploit to track or target a victim.[259] For instance, even if a victim's personal address is removed, their residential location could be revealed through records associated with a roommate.

To achieve this, brokers can employ the hashed identifiers from the central database as anchor points in their datasets to locate and address indirect or nonobvious data risks. By analyzing patterns and associations, such as shared addresses, linked phone numbers, or overlapping network connections, brokers can identify records indirectly tied to victims who have opted out. For example, if a hashed email address corresponds to a victim, brokers could identify other accounts registered at the same physical address or other individuals linked through shared data points. The FTC should establish clear, actionable thresholds for clustering proximity, ensuring that brokers strike a balance between privacy and technical feasibility without overreaching into unrelated data.

Placing the burden of identifying and removing indirect data on brokers is both practical and justified. Brokers have unparalleled access to vast quantities of data, advanced analytical tools, and the technical expertise required to perform this task. Victims, in contrast, lack both the resources and the visibility into the complex networks of data maintained by brokers. Moreover, brokers already use sophisticated clustering techniques for commercial purposes, such as building consumer profiles and linking related data across datasets.[260] Applying similar methods to identify indirect information tied to victims is not only feasible but also ethically imperative given their role in undercutting victim obscurity.

Brokers must also ensure that removed information does not reenter their systems. Newly ingested datasets must be automatically compared against hashed identifiers already in their possession. If a match with previously removed information is detected, the system must trigger automatic obscurity workflows and notify the central database. This ensures ongoing compliance and protects victims from reemerging risks over time.

---

256. Jake Frankenfield, *Personally Identifiable Information (PII): Definition, Types, and Examples*, INVESTOPEDIA (Nov. 2, 2023), https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp.

257. *See* Kadri, *supra* note 2, at 138–39.

258. *See generally* Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555 (2020).

259. *See Understanding Identifiable Data*, TEACHERS COLL.: COLUM. UNIV., https://www.tc.columbia.edu/institutional-review-board/irb-blog/2020/understanding-identifiable-data-.

260 *See* OFF. OF OVERSIGHT & INVESTIGATIONS MAJORITY STAFF, COMM. ON COMMERCE, SCI. & TRANSP., A REVIEW OF THE DATA BROKER INDUS.: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MKTG. PURPOSES 23 (2013).

5. Deidentification Standards

While deletion of personal data is a powerful tool for achieving victim obscurity, it is not the only means of protecting individuals. In some cases, deidentification serves as an alternative that balances the need to remove harmful personal data with the business interests of brokers. Deidentification must ensure that data is irreversibly unlinkable to any individual and incapable of reidentification through direct or indirect methods. [261] This requires adhering to rigorous benchmarks, such as differential privacy standards, which introduce controlled randomness to obscure individual data points while maintaining the statistical integrity of datasets. In reality, though, especially with machine learning, true deidentification is not always possible. The question becomes: how much deidentification does the law require?

By providing enforceable guidance on acceptable deidentification practices, the FTC can ensure consistency across the industry and account for technological advancements that might otherwise render older techniques obsolete. Given the unique context of brokered abuse, where abusers often possess intimate knowledge of their victims,[262] the standards must be designed with the utmost care. Well informed abusers may be able to reidentify information with fewer or less specific data points than the average person.[263] To close potential loopholes and prevent reidentification, brokers must ensure that deidentification is robust enough to foil the most dedicated and sophisticated abusers.

To verify compliance, the FTC should require periodic audits of broker deidentification methodologies.[264] To further streamline the process and improve compliance, the FTC could offer a centralized validation tool or API that brokers can use to test their deidentification methods against established benchmarks. This tool would ensure that deidentification practices are robust, consistent, and aligned with regulatory expectations, providing both accountability and operational clarity.

6. Standards Development Process

The development of technical standards for this framework is just as important as the implementation of the framework itself. A well-structured standards development process not only ensures the system's technical efficacy but also lends legitimacy and trust to its implementation. To this end, convening a diverse and knowledgeable standards-setting body is paramount. This body should include technical experts, privacy advocates, industry representatives, and FTC staff, ensuring a balanced approach that reflects the interests of all stakeholders while prioritizing victim protection and privacy. The technical community's work to mitigate the misuse of Apple AirTags for stalking highlights the importance of involving subject-matter experts. These experts bring critical insights into how technical design decisions impact real-world outcomes and can anticipate potential risks and challenges.

---

261. *See, e.g.*, Simson L. Garfinkel, *De-Identification of Personal Information,* NAT'L INST. STANDARDS & TECH., iii, 1 (2015) (defining de-identification as a "collection of approaches" to remove "identifying information from a dataset so that individual data cannot be linked with specific individuals").

262. *See* Kadri, *supra* note 2, at 138, 140–41 (showing how data brokers can fuel abuse with personal information, such as home addresses and even intimate images).

263. *See, e.g.*, Woodrow Hartzog & Ira S. Rubinstein, *Anonymization and Risk*, 91 WASH. L. REV. 703, 710–11.

264. *See, e.g.*, *Information for Data Brokers*, CAL. PRIVACY PROT. AGENCY, https://cppa.ca.gov/data_brokers.

Open standards must be adopted for API protocols, data formatting, clustering, deidentification, and cryptography to ensure cross-industry interoperability. The stakes for this process are particularly high given the immense resources and coordination required to build such a system. Once implemented, the framework will likely become entrenched, making significant redesigns or reversals exceedingly difficult. This reality underscores the importance of designing a solution that is robust and future-proof. An open, transparent, and inclusive standards development process safeguards against industry capture or arbitrage while ensuring that the system's design is robust, fair, and adaptable to future challenges.

IV. NEGOTIATING FIRST AMENDMENT CHALLENGES

> *"I believe that our concept of records and what needs to be public is not quite keeping up with the pace of technology. What these brokers are offering is not just something that you could go to the courthouse and get; it's like an aggregation of everything that I didn't necessarily provide[.]"*
> — Ella

Implementing a centralized obscurity system for abuse victims entails not only legislative and technical challenges but also constitutional ones. Even if legislators aspire to address brokered abuse, they might fear that constitutional doctrine will thwart their efforts. The regulation of information flows inevitably awakens the First Amendment Balrog.

Data brokers would have lawmakers and the public believe that laws—like the one proposed in this Article—regulating publicly available information face wholesale invalidation or at the very least must face strict scrutiny.[265] While this Part ultimately maintains that a centralized obscurity proposal should survive even under strict scrutiny, along the way it also complicates the seeming inevitability that laws regulating brokers' use of publicly available information must even clear such a hurdle.

First Amendment analysis can be broken into two cascading inquiries: *coverage* and *protection*.[266] The coverage inquiry determines whether the First Amendment is even in play when assessing a law's constitutionality, while the protection inquiry subsequently assesses the law's constitutionality.[267] Asserting that the First Amendment "covers" particular conduct means that First Amendment analysis is required to determine the constitutionality of a law regulating such conduct.[268] Asserting that the First Amendment "protects" such conduct means that the law is unconstitutional.[269] This Part begins by evaluating the coverage inquiry—casting skepticism on the presumption of First Amendment coverage for the regulation of brokers' sale of publicly available information—before moving to the protection inquiry to contemplate whether such speech, if covered, is commercial or noncommercial and therefore warrants protection under intermediate or strict scrutiny. Finally, this Part argues that this Article's proposed centralized obscurity system passes strict scrutiny despite its regulation of publicly available information.

---

265. Recht, *supra* note 25, at 4–7.

266. *See* Frederick Schauer, *Categories and the First Amendment: A Play in Three Acts*, 34 VAND. L. REV. 265, 267 (1981); Shanor, *supra* note 24, at 324–30.

267. Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L.J. 713, 714 (2000).

268. *Id*.

269. *Id.*

A. Constitutional Coverage: Data Brokers as Navigational Maps?

While the Supreme Court has explained that First Amendment coverage should adapt to evolving media of communication,[270] the data economy raises new questions about what activities the First Amendment covers.[271] The First Amendment does not cover all speech. As Robert Post theorizes, "First Amendment coverage is triggered by those forms of social interaction that realize First Amendment values . . . [and] extends to [media] that realize First Amendment values."[272] Scholars have spilled much ink over the animating values of free speech, often centering the protection of one of three general ideals:[273] (1) marketplace of ideas,[274] (2) individual autonomy,[275] (3) participatory democracy.[276] A First Amendment challenge to our centralized obscurity system, therefore, first raises the question of whether data brokerage represents a medium that realizes First Amendment values, and thus warrants coverage.

Why scrutinize First Amendment values rather than simply examine and apply First Amendment doctrine? First Amendment doctrine is notoriously incoherent,[277] and many view this incoherence as a product of doctrinal divergence from animating First Amendment values.[278] A more elemental inquiry is warranted before presuming First Amendment doctrine extends coverage to brokers' platforms as new media of communication.[279]

Regardless of where one locates free-speech values, "listener-based educative theory underlies much First Amendment doctrine."[280] In the context of regulating brokers, listeners' rights are particularly salient. Listeners' rights go hand in hand with access to

---

270. Brown v. Entertainment Merchants Assn., 564 U.S. 786, 790 (2011) (quoting Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 503 (1952)).

271. *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1150 (2005).

272. Post, *supra* note267, at 716.

273. *See* Tsesis, *supra* note 220, at 216.

274. Born from Justice Oliver Wendell Holmes's canonical dissent in *Abrams v. United States*, the "marketplace of ideas" theory of free speech champions the "free trade in ideas" as the premier driver of truth in a society predicated upon democratic self-government.250 U.S. 616, 630 (1919). While some scholars support Justice Holmes's view, others raise concerns about the theory's blind spots. *See* Eugene Volokh, *In Defense of the Marketplace of Ideas / Search for Truth as a Theory of Free Speech Protection*, 97 VA. L. REV. 595 (2011); Vincent A. Blasi, *Holmes and the Marketplace of Ideas*, 2004 SUP. CT. REV. 1 (2005).

275. *See* C. EDWIN BAKER, HUMAN LIBERTY AND FREEDOM OF SPEECH 47–69 (1992) (arguing that speech is protected because it "promotes both the speaker's self-fulfillment and the speaker's ability to participate in change"); Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 879 (1963) (explaining freedom of expression's role in "the achievement of self-realization").

276. This Article focuses on a participatory democracy theory of free speech rather than the broader democratic self-governance theory. Robert Post complicates the democratic self-governance theory by introducing his own nuanced, offshoot of the theory rooted in participatory democracy. *See* Robert Post, *Participatory Democracy and Free Speech*, 97 VA. L. REV. 477, 478 (2011). While democratic self-governance and participatory democracy may seem interchangeable, Post distinguishes between a Meiklejohnian view of democratic self-governance and his own theory of participatory democracy. *See* Robert Post, *Reconciling Theory and Doctrine in First Amendment Jurisprudence*, 88 CALIF. L. REV. 2353, 2368–2369 (2000) [hereinafter, Post, *Reconciling Theory and Doctrine*].

277. *See* Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249, 1249–50 (1995); Shanor, *supra* note 24, at 322–23.

278. *See* Post, *Reconciling Theory and* Doctrine, *supra* note 276, at 2365.

279. *See* Reno v. Am. C.L. Union, 521 U.S. 844, 885 (1997); Packingham v. North Carolina, 582 U.S. 98, 107–08 (2017).

280. Thomas E. Kadri, *Drawing Trump Naked: Curbing the Right of Publicity to Protect Public Discourse*, 78 MD. L. REV. 899, 917 (2019).

information,[281] and data brokers market themselves as the keyholders to the Library of Alexandria.[282] However, marketplace-of-ideas and participatory-democracy theories of free speech view listeners' rights in meaningfully different ways that affect the coverage inquiry.

Jane Bambauer contends that data's potential to inform justifies its classification as speech.[283] According to Bambauer, the coverage question is not whether data is speech in a metaphysical sense, but rather whether the regulation "deliberately interfere[s] with an individual's effort to learn something new."[284] In her view, First Amendment coverage should extend to laws that "target[] information-gathering for the very purpose of disrupting it."[285] While some courts have effectively adopted this view,[286] this coverage analysis arguably privileges a particularly expansive marketplace-of-ideas theory,[287] often to the detriment of public discourse.[288]

Bambauer's scientific-method framing offers a compelling take on a marketplace-of-ideas theory, but courts might be concerned that it leads to coverage creep and sanitizes First Amendment values.[289] Regulating the public's access to information might not always trigger First Amendment scrutiny under a participatory-democracy view of the First Amendment. Post stresses the importance of the relationship between speaker and listener.[290] To truly serve First Amendment values, he argues, media of communication must do more than "facilitate the communication of particularized messages," and "the facilitation of communication is not by itself a sufficient reason for social conventions to be valued by the First Amendment."[291] Under a Postian participatory-democracy theory of

---

281. *See id.* at 912–17; Leslie Kendrick, *Are Speech Rights for Speakers?*, 103 VA. L. REV. 1767, 1789 (2017); Meir Dan-Cohen, *Freedoms of Collective Speech: A Theory of Protected Communications by Organizations, Communities, and the State*, 79 CALIF. L. REV. 1229, 1233 (1991); Morgan N. Weiland, *Expanding the Periphery and Threatening the Core: The Ascendant Libertarian Speech Tradition*, 69 STAN. L. REV. 1389, 1451 (2017).

282. *See* Matthew Crain, *The Limits of Transparency: Data Brokers and Commodification*, 20 NEW MEDIA & SOC'Y 1, 3 (2016).

283. Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 61 (2014).

284. *Id.* at 60.

285. Jane Bambauer, *The Empirical First Amendment*, 78 OHIO ST. L.J. 947, 955 (2017).

286. *See* Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 862–63 (2012); *see also, e.g.*, IMS Health Inc. v. Sorrell, 630 F.3d 263, 271–72 (2d Cir. 2010).

287. Bambauer's coverage analysis privileges a narrow view of the "marketplace of ideas" theory. Meiklejohn's approach to democratic self-governance is "quite analogous to the theory of the marketplace of ideas." Post, *Reconciling Theory and Doctrine*, *supra* note 276, at 2369. But Meiklejohn's approach foregrounds the aphorism that "[w]hat is essential is not that everyone shall speak, but that everything worth saying shall be said." ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE 26 (1965). A Meiklejohnian approach aims to distinguish "between cognitive and noncognitive aspects of speech" and to extend "less constitutional protection" to the latter. Cass R. Sunstein, *Pornography and the First Amendment*, 1986 DUKE L.J. 589, 603 (1968).

288. For background on the concept of "public discourse" as an animating principle of the First Amendment, *see* ROBERT C. POST, CITIZENS DIVIDED: CAMPAIGN FINANCE REFORM AND THE CONSTITUTION 49 (2014) ("I shall use the term public discourse to describe the communicative processes by which persons participate in the formation of public opinion."); ROBERT C. POST, CONSTITUTIONAL DOMAINS: DEMOCRACY, COMMUNITY, MANAGEMENT 7 (1995) (defining public discourse as "an open structure of communication" in which there can be "reconciliation of individual and collective autonomy"); Post, *supra* note 276, at 621; Robert C. Post, *The Constitutional Status of Commercial Speech*, 48 UCLA L. REV. 1, 7 (2000) ("Public discourse is comprised of those processes of communication that must remain open to the participation of citizens if democratic legitimacy is to be maintained."); Robert C. Post, *Meiklejohn's Mistake: Individual Autonomy and the Reform of Public Discourse*, 64 U. COLO. L. REV. 1109, 1115–16 (using the term "public discourse" to refer to the "communicative processes sufficient to instill in citizens a sense of participation, legitimacy, and identification").

289. *See* Bambauer, *supra* note 285, at 948–950.

290. *See* Post, *supra* note 277, at 1254–55.

291. *Id.* at 1254.

free speech, data dossiers might not receive First Amendment protection. Akin to how navigation charts communicate "monologically to their audience," data brokers' dossiers speak monologically to their clientele of private parties.[292] Rote conveyance of personal data functions in a similar fashion to a map or other reference source. The consumer, or audience, "assume[s] a position of dependence" and relies on the data as unadulterated fact.[293] Facts are only "elements of speech."[294] Unless a speaker imbues such facts with an expressive or communicative "use" to express a message, facts alone might not constitute covered speech.[295] Data dossiers, like navigation charts, arguably function as products that lack the kinds of social interactions that realize First Amendment values.[296]

Rather than focusing narrowly on information flows, Post emphasizes the constitutional salience of public discourse.[297] This notion, too, could affect the coverage analysis for data brokerage. Drawing on Supreme Court doctrine,[298] Post raises the "paradox of public discourse,"[299] which posits that public discourse can only perform its constitutional function "if it is conducted with a modicum of civility."[300] Although demanding civility may constrain speech, sufficiently abusive and alienating public discourse could lead individuals to recoil from engaging in public discourse to influence the construction of public opinion.[301] If incivility is left to fester, public discourse will fail to foster a sense of legitimacy and participation, and the rationale for safeguarding the principle will wane.[302] It is precisely this line of thought that leads Post to the conclusion that the "right to be forgotten" is compatible with the democratic function of public discourse.[303]

Sometimes when you wield a constitutional hammer, everything looks like a nail. And no constitutional right possesses more social and rhetorical power than the First Amendment and freedom of speech.[304] Frederick Schauer refers to this phenomenon as First Amendment magnetism.[305] First Amendment magnetism characterizes the "accelerating attempt to widen the scope of First Amendment coverage to include actions and events traditionally thought to be far removed from any plausible conception of the purposes of a principles of free speech."[306] However, in an age of rapid First Amendment expansionism, some courts might scrutinize the coverage question to avoid First Amendment creep that operates as a deregulatory tool.[307]

---

292. *Id.* at 1254 (invoking navigation charts as an example of media that communicate particularized messages that do not get First Amendment protection).

293. *Id.*

294. Rumsfeld v. Forum for Academic & Institutional Rights, 547 U.S. 47, 61–62 (2006).

295. *See* Spence v. Washington, 418 U.S. 405, 409–10 (1974).

296. *Cf.* Post, *supra* note 277, at 1253–55 (1995); *see also* Ashutosh Bhagwat, *Details: Specific Facts and the First Amendment*, 86 S. CAL. L. REV. 1, 40 (2012) ("[W]hile personal details sometimes play a key role in forms of self-governance, the relationship is often far more distant.").

297. *See* Post, *Reconciling Theory and Doctrine*, *supra* note 276, at 2371–72.

298. Boos v. Barry, 485 U.S. 312, 322 (1988) (O'Connor, J., plurality opinion) (quoting *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 56 (1988)).

299. *See* Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, The Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 1009 (2018).

300. *Id*.

301. Kadri, *supra* note 280, at 948–49.

302. *Id.*

303. *See* Post, *supra* note 299, at 1008–09.

304. *See* Frederick Schauer, *Boundaries of the First Amendment*, 117 HARV. L. REV. 1765, 1790 (2004).

305. *Id.*

306. Schauer, *supra* note 24, at 1617.

307. *See* Shanor, *supra* note 24, at 322.

It is precisely these deregulatory "perils of Volokhner" that underpin Neil Richards's contention that privacy regulation and speech regulation need not be in tension.[308] Richards challenges the assumption that information flows constitute speech and therefore fall within the ambit of the First Amendment.[309] In his view, such an absolutist approach to First Amendment coverage fails to adequately question the "constitutional metaphysics of 'speech.'"[310] Calling "things 'speech' or 'not speech'" might spike judicial anxiety,[311] but courts might be persuaded by the chorus of scholars calling on them to police the boundaries of coverage given the First Amendment's deregulatory expansion.[312] While privacy must be squared with First Amendment interests, privacy often gets the short end of the stick.[313]

First Amendment questions raised by the digital age invite us to set aside our casebooks and let more elemental constitutional inquiries come to the fore.[314] Even if some contemporary doctrine suggests that data dossiers might be covered, courts should interrogate whether such a conclusion serves the First Amendment's animating values. Laws like the one proposed in this Article force us to reckon with the costs of First Amendment expansionism, yet they might also provide an opportunity to pump the brakes and demand greater introspection on how constitutional coverage reflects socio-constitutional values.

B. Constitutional Protection: The Commerciality Conundrum

Given the rapid expansion of First Amendment coverage,[315] courts may well extend coverage to data brokers' sites. Presuming coverage, the protection inquiry begins. Before assessing the constitutionality of a law regulating the dissemination of abuse victims' data, courts would need to determine the proper level of constitutional scrutiny. If they deem the dissemination of abuse victims' data to be non-commercial speech, the law must survive strict scrutiny rather than the intermediate scrutiny applied to commercial speech.[316]

1. Commercial Speech: Dossiers v. News

Historically, the First Amendment did not protect commercial speech.[317] However, the Court determined in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.* that commercial speech warrants constitutional protection, albeit lesser protection than noncommercial speech.[318] The Court laid out the contours of this diminished protection in *Central Hudson*, articulating a four-part test.[319] First, commercial speech "must concern lawful activity and not be misleading."[320] If the speech clears this initial threshold, then the state may only regulate if (1) the "government interest is

308. *See* Richards, *supra* note 271, at 1166 (criticizing the deregulatory effect of First Amendment arguments advanced by Eugene Volokh).

309. *Id.* at 1169.

310. *Id.* at 1168.

311. *Id.* at 1171.

312. *See* Shanor, *supra* note 24, at 322; Post & Shanor, *supra* note 24, at 166–67.

313. Richards, *supra* note 271, at 1179.

314. *See* Schauer, *supra* note 304, at 1777–78.

315. *See* Shanor, *supra* note 24, at 322.

316. *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm., 447 U.S. 557, 562–64 (1980).

317. *See* Valentine v. Chrestensen, 316 U.S. 52, 54 (1942) ("[T]he Constitution imposes no such restraint on government as respects purely commercial advertising.").

318. *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 770–71 (1976).

319. *See Central Hudson*, 447 U.S. at 566.

320. *Id.*

substantial," (2) the regulation "directly advances the governmental interest asserted," and (3) the regulation is "not more extensive than is necessary to serve that interest."[321] While the Court in *Sorrell v. IMS Health* hinted at heightened scrutiny for content and view-based regulation of data flows,[322] the Court's silence on the contours of this heightened scrutiny has led lower courts often to continue to apply a version of the *Central Hudson* test.[323]

Meanwhile, noncommercial speech is at the core of canonically protected speech and once information has entered the public sphere, the First Amendment generally precludes the government from restricting its subsequent use.[324] Once information had been "publicly revealed"[325] and "widely disseminated"[326] to the general public, it became unconstitutional to "restrain its dissemination"[327] and retract it from the "public domain."[328] Orin Kerr likens this phenomenon to "publishing a newspaper but then forbidding someone to read it."[329]

Cox Broadcasting Corporation v. Cohn[330] and *Florida Star v. B.J.F.*[331] present two cases where courts initially held news outlets liable for publishing crime victims' names.[332] In *Cox*, the television station broadcast a rape and murder victim's name that court records had already "publicly revealed,"[333] while the newspaper in *Florida Star* published a rape victim's name derived from a "publicly released police report."[334] In both cases, the Court held that after the information entered "the public domain," the First Amendment protected the use of that information."[335]

The Court came to a similar conclusion in *Smith v. Daily Mail Publishing Company*[336] where the information came from a nongovernmental source. In *Smith*, two reporters learned the name of a teenage boy who killed his classmate from individuals present at the crime scene.[337] Following the airing of the boy's name by several radio stations, newspapers printed the name and were indicted under a state law that made it a crime to publish the names of juvenile arrestees without a court's written approval.[338] The Court held that the First Amendment prohibited the state from punishing the publication of the

321. *Id.*

322. *See* Sorrell v. IMS Health, 564 U.S. 552, 570 (2011); Bhagwat, *supra* note 286, at 859–60.

323. *See* Robert L. Kerr, *Desperately Seeking Coherence: The Lower Courts Struggle to Determine the Meaning of Sorrell for the Commercial Speech Doctrine*, 7 U. BALT. J. MED. L & ETHICS 1, 4 (2019).

324. *Cf.* Eugene Volokh, *No Take-Backs, No Do-Overs, No Data Replevin*, VOLOKH CONSPIRACY (June 13, 2019, 5:27 PM), https://reason.com/2019/06/13/no-take-backs-no-do-overs-no-data-replevin [https://perma.cc/VC7L-Z344] (remarking on a case where the court held that the plaintiff couldn't rely on the remedy of replevin to "take back" what he already said in a digital recording).

325. Cox Broad. Corp. v. Cohn, 420 U.S. 469, 471 (1975).

326. Okla. Publ'g Co. v. Okla. Cnty. Dist. Ct., 430 U.S. 308, 310 (1977) (per curiam).

327. Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979).

328. Fla. Star v. B.J.F., 491 U.S. 524, 538 (1989).

329. Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1169 (2016).

330. 420 U.S. 469 (1975).

331. 491 U.S. 524 (1989).

332. *Cox Broad. Corp.*, 420 U.S. at 471, 474 (assessing the constitutionality of imposing civil liability under a state law recognizing tortious invasion of privacy); *Fla. Star*, 491 U.S. at 526 (quoting FLA. STAT. § 794.03 (1987)) (assessing the constitutionality of imposing civil liability under a state law making it illegal to "print, publish, or broadcast" the names of victims of sexual offenses).

333. *Cox*, 420 U.S. at 471, 473–74.

334. *Fla. Star*, 491 U.S. at 526–27.

335. *Cox*, 420 U.S. at 495–96 (finding that the information entered the "the public domain" because the records containing the information were "open to public inspection" and had been "released to the public"); *Fla. Star*, 491 U.S. at 527, 532, 538 (determining that because the department did not "restrict access either to the pressroom or to the reports made available therein" the information entered "the public domain").

336. 443 U.S. 97 (1979).

337. *See id.*, at 99.

338. *See id.* at 99–100.

information.[339] Despite recognizing prior cases involved the governmental release of information, the Court downplayed this distinction, explaining that the public "cannot be made to rely solely upon the sufferance of government to supply it with information."[340] The information's source did not matter as much as the fact that the information had already entered the public domain.[341]

Now, as applied to this Article's proposed centralized obscurity system, does data brokers' commercial dissemination of personal data warrant protection as commercial speech or noncommercial speech? Ultimately, this discussion hinges in many ways on whether data brokers really serve a newsgathering function that informs the public. On its face, this determination may appear facile. Data brokers represent a new medium of communication that collects information from public and private sources and collates that information for effortless consumption. Do they charge for access to this information? Yes, but so does the New York Times and countless other publications. Therefore, as new media of communication that serve a newsgathering function, data brokers' sale of personal information would seem to receive noncommercial speech protection akin to newspapers.

However, does the private sale of dossiers really qualify as a journalistic endeavor? Insofar as private dossiers have the potential to inform, they seem to do so within the bounds of the commercial speech doctrine. At its core, the distinction between public discourse and commercial speech rests upon a commonsense evaluation as to whether "the utterance of a particular speaker should be understood as an effort to engage public opinion or instead simply to sell products."[342] The court in *Brooks v. Thomson Reuters Corp.*[343] addressed this very question as it relates to data broker dossiers:

> Here, by contrast, Thomson Reuters is not a journalist performing a 'public benefit' by making Plaintiffs' personal information available to the public. Rather, the company's dissemination of this information only benefits the private parties who purchase the CLEAR dossiers. All the other cases cited by Thomson Reuters to suggest that there is no privacy right in speech derived from public records are similarly inapposite because they involve *journalists* disclosing publicly available information *to the general public*.[344]

The court draws a clear distinction between data dossiers for the benefit of private parties and journalists disclosing publicly available information to the general public.[345] Data brokers' central purpose is to sell a product—dossiers—to private parties, not to engage public opinion as a journalistic purveyor of information. The Supreme Court made a similar distinction in *Dun and Bradstreet, Inc. v. Greenmoss Builders, Inc.*,[346] where a nonmedia information distributor sought the same First Amendment protections as media defendants in defamation actions.[347] The Court found that the sale of credit reports was "speech solely in the individual interest of the speaker and its specific business audience"

339. *See id.* at 104 (1979).
340. *Id.* at 104.
341. *See id.*
342. Robert C. Post, *The Constitutional Status of Commercial Speech*, 48 UCLA L. REV. 1, 18 (2000).
343. 21-CV-01418, 2021 WL 3621837 (N.D. Cal. Aug. 16, 2021).
344. *Id.* at *9 (N.D. Cal. Aug. 16, 2021).
345. *Id.*
346. 472 U.S. 749 (1985).
347 *See id.* at 753.

and was "solely motivated by the desire for profit."[348] Therefore, the speech did not address a matter of public concern and only received the diminished protection afforded to commercial speech.[349] Similarly here, data brokers—the largest of which are credit reporting agencies[350]—sell dossiers purely from a place of monetary, self-interest.[351] Utilizing public discourse as a rhetorical front, data brokers meddle away at their sordid craft of laundering informational currency into sovereign currency.[352] Common sense counsels us to look past the journalistic façade and into the dimly lit backroom where the ignoble gains are tallied, tracked, and traded.

Despite the broker industry's claims to the contrary, it is anything but clear that data brokers should receive noncommercial speech protection rather than the diminished protection afforded to commercial speech.

2. Non-Commercial Speech: Passing Strict Scrutiny

Even if courts determine that data brokers' dissemination of abuse victims' information—especially publicly collected information—should undergo strict scrutiny, this Article's centralized obscurity system proposal passes this heightened scrutiny.

To pass strict scrutiny, the government must first demonstrate a compelling government interest.[353] Public health and safety is a classic example of a compelling government interest,[354] and the protection of abuse victims from the primary harms of brokered abuse certainly fit within the ambit of these core governmental concerns.[355]

The government also has a compelling interest in protecting victims from the secondary harms of brokered abuse, particularly the chilling effect of withdrawing from the public sphere. Too often the diminished First Amendment rights of victims go unnoticed. Nowhere is privacy and personal freedom more intertwined than marginalized communities.[356] While data privacy regulation may implicate the First Amendment rights of data brokers and those who benefit from the commercial information economy, it also implicates the First Amendment rights of abuse victims who suffer the chilling effect of withdrawing from society in the hope of securing physical and emotional safety.[357]

---

348. *Id,* at 762.

349. *See id*.

350. *See* Justin Sherman, *Credit Reporting Agencies Don't Just Report Credit Scores*, DUKE SANFORD SCHOOL OF PUB. POL'Y (Nov. 9, 2022), https://techpolicy.sanford.duke.edu/blogroll/credit-reporting-agencies-dont-just-report-credit-scores.

351. *See* ELEC. PRIVACY INFO. CTR., *Data Brokers*, https://epic.org/issues/consumer-privacy/data-brokers ("For these companies, consumers are the product, not the customer.").

352. *See* Ayoub & Gotein, *supra* note 53.

353. *See, e.g.*, Austin v. Mich. Chamber of Com., 494 U.S. 652, 655 (1990).

354. *See* J. Morris Clark, *Guidelines for the Free Exercise Clause*, 83 HARV. L. REV. 327, 330–31 (1969) ("The purpose of almost any law can be traced back to one or another of the fundamental concerns of government: public health and safety, public peace and order, defense, revenue.").

355. *See* Part I.B.1.

356. *See* SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS 8 (2020); *see also* Faye Vasilopoulos, *Hanging by A Thread: Meta's New Platform, Threads, Sheds Light on the Slow Unraveling of Individual Privacy*, 58 U. ILL. CHI. L. REV. 473, 482 (2024).

357. *See* Danielle Keats Citron & Jonathon W. Penney, *When Law Frees Us to Speak*, 87 FORDHAM L. REV. 2317, 2318 (2019); *see also* Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1478 (2022); Mary Anne Franks, *Free Speech Black Hole: Can the Internet Escape the Gravitational Pull of the First Amendment?*, KNIGHT FIRST AMEND. INST. COLUM. U. (Aug. 21, 2019), https://knightcolumbia.org/content/the-free-speech-black-hole-can-the-internet-escape-the-gravitational-pull-of-the-first-amendment.

The "paradox of public discourse"[358] highlights the need for civility to safeguard the democratic values underpinning the First Amendment. For abuse victims, privacy is a necessary precondition for self-expression.[359] "The fight for intimate privacy is the fight for free speech."[360] While the First Amendment does not generally employ balancing,[361] it is difficult to ignore the competing First Amendment interests at play and their respective significance as it relates to democratic self-governance values.[362] And there is little question as to whether data broker sites degrade democratic self-governance values. Many abuse victims refrain from voting—*the* fundamental right undergirding participatory democracy—for fear that data brokers will scrape their information from public voting rolls and make them readily accessible to their abusers at a negligible expense.[363] There is arguably no greater governmental interest than ensuring all citizens, especially vulnerable ones, exercise their right to vote. Ultimately, a strict scrutiny analysis will likely hinge on whether the regulation is narrowly tailored rather than whether a compelling government interest exists,[364] but it is vital to foreground the stakes at play here.

The centralized obscurity system not only must advance a compelling governmental interest, but it also must be narrowly tailored. The proposal, therefore, should meaningfully shield victims from the harms of brokered abuse in the least speech restrictive manner. Accordingly, the regulation must stand up to brokers' challenges that it is both overinclusive and underinclusive.[365]

Brokers likely will argue that the proposal is overinclusive—that the government restricts more speech than necessary to advance its aim of protecting abuse victims from brokered abuse. Brokers may point to the broad definitions of "data broker" and "covered data" to demonstrate the overinclusive sweep of the regulation. While it is true that the proposal includes seemingly broad definitions, it does so to effectively achieve the aim of protecting domestic abuse victims from brokered abuse. To ensure abuse victims' safety, the regulation must adopt a definition of "data broker" that captures the entire supply chain

---

358. Post, *supra* note 299, at 1009; Robert Post, *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and* Hustler Magazine v. Falwell, 103 HARV. L. REV. 601, 640–44, 680–84 (1990).

359. *Cf.* Danielle Keats Citron, *Intimate Privacy's Protection Enables Free Speech*, 2 J. FREE SPEECH L. 3, 3 (2022) ("[I]ntimate privacy is an essential precondition for self-expression.").

360. *Id*. at 4.

361. In the limited employer-employee context, the Court utilizes the Pickering test. *See* Rankin v. McPherson, 483 U.S. 378, 384–85 (1987) (quoting Pickering v. Bd. of Educ., 391 U.S. 563, 568 (1968)); *see also* Anna Tichy, Gillis v. Miller, 64 N.Y.L. SCH. L. REV. 115, 129 (2020); Abby Ward, *In Defense of* Pickering*: When A Public Employee's Social Media Speech, Particularly Political Speech, Conflicts with Their Employer's Public Service*, 108 MINN. L. REV. 1643, 1700 (2024).

362. *See* Scott Skinner-Thompson, *Agonistic Privacy & Equitable Democracy*, 131 YALE L.J.F. 454, 456 (2021) ("Although visibility comes with risks for members of marginalized groups, controlled visibility through privacy protections has the potential to serve important antisubordination goals and lead to broader societal participation of entire communities in the public square. Given that public space may deny the existence of nonnormative identities, that participation may by itself be radical and politically transformative."); *see also* Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 430 (2017) ("A democratic conception of privacy, by emphasizing the experiences of those most vulnerable to its violation, offers the best chance of securing privacy for all.").

363. *See* Scottie Andrew, *For Abuse Victims, Registering to Vote Brings a Dangerous Tradeoff*, CNN (Oct. 27, 2020, 3:57 PM), https://www.cnn.com/2020/10/27/us/domestic-violence-voting-election-privacy-trnd/index.html; *see also* Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, WIS. L. REV. 861, 896–97 (2014) (claiming that a breach of political data results in harms such as a declining faith in publicly supervised political processes).

364. When arguing that New Jersey's Daniel's Law violated the First Amendment, the class of data brokers did not even bother to challenge whether the government had a compelling interest. *See* Brief for Plaintiffs' Memorandum of Law in Opposition to Defendants' Consol. Motion to Dismiss at 41–42, Atlas Data Priv. Corp. v. We Inform, LLC, 2024 WL 4905924 (D.N.J. Nov. 26, 2024) (No. CV 24-10600) [hereinafter *Atlas Data Privacy Brief*].

365. *Cf. id.* at 28, 31–34.

to prevent loopholes that may lead to data leakage. The possible consequence of such a leak for abuse victims warrants more sweeping coverage. The same logic applies to "covered data," where indirect data such as a roommate's data may allow determined abusers to locate victims through a proxy. Therefore, a more expansive definition of "covered data" is vital to effectively safeguarding abuse victims from their abusers. Otherwise, workarounds leave abuse victims at continued risk.

The regulation's verification requirement and aggregated, deidentified data carveout also significantly limit the sweep of the proposal. Brokers have raised the lack of verification requirements to argue existing non-disclosure laws are overinclusive.[366] This Article's proposal, however, limits access to the centralized obscurity system remedy in two ways. First, the proposal limits protected persons to those who have experienced abuse as defined by the VAWA along with additionally enumerated forms of abuse not comprehensively covered by the VAWA, such as stalking.[367] Second, the proposal implements a self-attestation regime where victims submit sworn statements affirming their eligibility to access the centralized obscurity system. This dual-layered approach balances the competing need to provide abuse victims unencumbered access to the centralized obscurity system's protections while also ensuring the system adequately limits this obscurity remedy to abuse victims. The proposal also limits covered data to PII, carving-out aggregated, deidentified data entirely. Bulk, deidentified transactions do not meaningfully implicate abuse victims' safety and they are core to the lucrative marketing and advertising data economy. Therefore, the proposal covers data that meaningfully implicates abuse victim safety while balancing the business interests of brokers.

Brokers have also argued that laws solely regulating commercial disclosures of personal data are underinclusive because public agencies can often still disclose the same covered personal data.[368] While this Article's centralized obscurity system may not cover all governmental disclosures of covered personal data, a regulation need not be perfectly tailored to pass strict scrutiny.[369] Here, the functional aim of the regulation is practical obscurity[370] for abuse victims. Fundamentally, data brokers provide frictionless personal data dossiers as a service. The same publicly available personal data may be accessed through FOIA requests, but such processes require tailored requests—often requiring specification of the desired data and the agency that should field the request—and take time to process. Convenience is as central to the product as the data itself. The regulation does not strive to prevent all access to abuse victims' data but rather stem the tide of abuse, and re-abuse, that arises from instantaneous digital access to troves of frequently refreshed personal data at the click of button for a nominal expense.

The Supreme Court recognizes the significance of practical obscurity, coining the term itself in *United States Department of Justice v. Reporters Committee for Freedom of the*

366. *See id.* at 32 ("[w]hether the statute contains a verification requirement does not alter the scope of its coverage or the amount of speech it restricts.").

367. *See supra* Part III.B.1.

368. *See Atlas Data Privacy Brief* at 33–36.

369. *See* Burson v. Freeman, 504 U.S. 191, 209 (1992) (plurality opinion); *see also* Bd. of Trs. of the State Univ. of N.Y. v. Fox, 492 U.S. 469, 480 (1989) ("What our decisions require is . . . a fit that is not necessarily perfect, but reasonable . . . ."); Matthew Passalacqua, *Something's Brewing Within the Commercial Speech Doctrine*, 46 VAL. U. L. REV. 607, 642 (2012).

370. Practical obscurity describes the functionally obscure state of scattered, uncollated, and non-computerized information in contrast to streamlined, digital access to that very same information in an aggregated form. *See* Nancy Marder, *From "Practical Obscurity" to Web Disclosure: A New Understanding of Public Information*, 59 SYRACUSE L. REV. 441, 441–43 (2009).

Press.[371] Writing for the Court, Justice Stevens shared Ella's concern about the new age of instantaneous access to collated public information: "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[372] In recognizing this, the Court seems to consider the medium of dissemination to be as important as the information itself when determining whether "the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information."[373] The question is less about the limitation of access to public information and more about the ease of access. Similarly, here, while the regulation would still allow for targeted data requests from public agencies, this reversion to practical obscurity status quo—where discrete information must be accessed through FOIA requests to specific public agencies—materially advances the government's compelling interest of protecting victims from brokered abuse.

CONCLUSION

Brokered abuse represents a fundamental failure of privacy law—an abdication of policymaker responsibility to prioritize human safety over corporate profit. Victims of abuse should not have to navigate an insurmountable maze of data broker opt-out processes to achieve the basic security of online obscurity. This Article underscores the urgent need for an enforceable, centralized obscurity system that redistributes the burden of achieving obscurity from victims to the data brokers profiting off their vulnerability. By mandating a streamlined, comprehensive obscurity system that leverages data broker insight into the informational ecosystem and sophisticated data processing technologies, regulatory intervention can provide a sustainable solution that ensures victim safety without retraumatizing them.

However, any regulatory intervention must be designed with constitutional resilience in mind, particularly in the face of inevitable First Amendment challenges. The broker industry will certainly argue that restrictions on the dissemination of data dossiers, particularly their publicly available components, violate their right to free speech. To ensure a legally durable regulatory solution to brokered abuse, policymakers must craft a system that is narrowly tailored to achieve the compelling government interest of protecting individuals from stalking, harassment, and violence.

Looking ahead, the future of privacy law must center victims. Without immediate action, the cycle of harm will only deepen, leaving countless individuals at risk. The implications of inaction extend beyond individual victims to society at large, as the erosion of privacy threatens the very principles of autonomy, security, and participatory democracy. The fight for privacy is, at its core, a fight for dignity, safety, and human rights—one that demands immediate and uncompromising legal reform.

---

371. *See* United States Dep't of Just. v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 762–64 (1989).
372. *Id.* at 764.
373. *Id.*