10

Brokered Abuse

*Thomas E. Kadri**

10.1 INTRODUCTION

It's accually obsene what you can find out about a person on the internet.[1]

To some, this typo-ridden remark might sound banal. We know that our data drifts around online, with digital flotsam and jetsam washing up sporadically on different websites across the internet. Surveillance has been so normalized that, these days, many people aren't distressed when their information appears in a Google search, even if they sometimes fret about their privacy in other settings.

But this remark is not a throwaway line by a disgruntled netizen. No. It's a boast by a stalker, Liam Youens, who went online to find his victim, Amy Boyer. Youens traced Boyer after buying her work address from a data broker – a company that traffics information about people for profit. Youens documented his search for Boyer's whereabouts on his personal website: "I found an internet site to do that, and to my surprize everything else under the Sun. Most importantly: her current employment."[2] After he asked the broker for more information, he just had to bide his time. "I'm waiting for the results," he wrote ominously, not long before shooting Boyer dead at work.[3]

* Huge thanks to RonNell Andersen Jones, Elettra Bietti, Hannah Bloch-Wehba, Sarah Burns, Ryan Calo, Ignacio Cofone, Julie Cohen, Amy Gajda, Yael Grauer, Nikolas Guggenberger, Woodrow Hartzog, Mike Hintze, Leigh Honeywell, Ido Kilovaty, Anne Klinefelter, Kyle Langvardt, Mark Lemley, Lyrissa Lidsky, Christopher Morten, Paul Ohm, Natália Pires de Vasconcelos, Ani Satz, Evan Selinger, Scott Skinner-Thompson, Eugene Volokh, Rachel Vrabec, Ari Waldman, Rebecca Wexler, Felix Wu, and participants at the Privacy Law Scholars Conference and the UGA-Emory Faculty Workshop. I dedicate this chapter to the clients and volunteers at the Clinic to End Tech Abuse.

[1] *Greetings Infidels, I Am Liam Youens*, https://perma.cc/TPY7-JCGA.

[2] *Id.*

[3] *Id.*; Kaveh Waddell, *How FamilyTreeNow Makes Stalking Easy*, ATLANTIC (Jan. 17, 2017), https://perma.cc/H6AG-CHSE.

Data brokers fuel abuse by sharing people's information and thwarting their obscurity. The value of obscurity, though sometimes overlooked in privacy discourse, rests on the idea that "information is safe – at least to some degree – when it is hard to obtain or understand."[4] Brokers hinder obscurity by making it easier and likelier to find or fathom information about people. This act of foiling obscurity, in turn, facilitates interpersonal abuse. The physical violence suffered by Amy Boyer is but one kind of abuse; people also face stalking, harassment, doxing, defamation, fraud, sextortion, and nonconsensual sharing of their intimate images.[5]

This chapter explores the phenomenon of *brokered abuse*: the ways that data brokerage enables and exacerbates interpersonal abuse. The harms of brokered abuse go beyond the fact that brokers make it easier to surveil people and expose them to physical, psychological, financial, and reputational harms. In addition, people must beg every single broker to conceal their information from thousands of separate databases, over and over again, with little or no legal recourse if brokers reject their efforts to regain some obscurity. Due partly to existing laws, this whack-a-mole burden of repeatedly pleading to obscure data can trigger trauma and distress. Only by grasping this fuller scope of brokered abuse can we begin to regulate it.[6]

This chapter splits into three sections. Section 10.2 introduces the broker industry before Section 10.3 reveals how the law largely fails to address, and is even complicit in, key features of brokered abuse. Section 10.4 then explores the harms stemming from brokered abuse in order to lay some foundations for regulating them.

10.2 DATA BROKERS AS INFORMATION TRAFFICKERS

Data brokerage is a multibillion-dollar industry.[7] Thousands of companies form a sprawling network of brokers that buy, sell, trade, and license gigabytes of human information. Though brokers' business models vary, their power and profit fundamentally stem from trafficking information about people.[8]

[4] Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* Spaces for the Future: A Companion to Philosophy of Technology 119, 119 (Joseph Pitt & Ashley Shew eds., 2018).

[5] *See* Danielle Keats Citron, *Sexual Privacy*, 128 Yale L.J. 1870 (2019) (discussing how networked technologies have facilitated various forms of interpersonal abuse).

[6] *See* Thomas E. Kadri, *Networks of Empathy*, 2020 Utah L. Rev. 1075, 1075 (urging that "[w]e can neither understand nor address digital abuse unless we view technology in a deeper social context and grapple with how and why digital abuse is harmful").

[7] Salome Viljoen, *A Relational Theory of Data Governance*, 131 Yale L.J. 573, 588 n.19 (2021) (observing that "[s]ome evidence pegs the global data-brokerage industry at about $200 billion annually").

[8] *See* Neil Richards, Why Privacy Matters 1–11 (2022) (connecting privacy, power, and "human information" and defining privacy as "the degree to which human information is neither known nor used"). For important early scholarship on brokers, *see* 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); Daniel J. Solove &

https://doi.org/10.1017/9781009174411.013 Published online by Cambridge University Press

For the most part, brokers buy information from other companies and gather it from government records and public websites.[9] From there, brokers build profiles including data like a person's name, aliases, photos, gender, birthdate, citizenship, religion, addresses, phone numbers, social-media accounts, email addresses, Social Security number, employers, schools, families, cohabitants, purchases, health conditions, and hobbies. These data dossiers are then sold for a fee or even shared for "free" thanks to the ads adorning broker websites.[10]

There are, to be fair, some benefits tied to the broker industry.[11] Transparency and accessibility come from publicizing information online, including data drawn from public records. Journalists, activists, academics, and the general public can garner insights from this information.[12] Indeed, a person might even evade interpersonal abuse or other ills after discovering an acquaintance's restraining order or criminal record through a broker. Though this kind of data is often accessible in other ways, a Google search is easier, faster, and cheaper than a trip to the county courthouse.[13]

Some people also use brokers to locate heirs or reconnect with long-lost friends and family. Others might rely on brokered data to inform their hiring decisions. Some companies rely on brokers in order to collect debts or discover fraud, corroborating information given to them by a customer or client. And brokers can even assist the legal system, such as when class-action awards are being distributed. These perks cannot be ignored, but we should be wary of their value being exaggerated.

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), https://perma.cc/34YR-A5LN.

[9] *See* Margaret B. Kwoka, *FOIA, Inc.*, 65 Duke L.J. 1361, 1376–401 (2016) (detailing how a vast industry of "information resellers" requests federal public records under the Freedom of Information Act (FOIA) and resells them for profit); David E. Pozen, *Transparency's Ideological Drift*, 128 Yale L.J. 100, 125 (2018) (observing that "commercial requesters – including a cottage industry of data brokers and information resellers – submit over two-thirds" of FOIA requests to various federal agencies).

[10] *See* Amy Gajda, Seek and Hide: The Tangled History of the Right to Privacy 231–41 (2022) (discussing the extensive data dossiers compiled by brokers and other companies).

[11] *See generally* Jennifer Barrett Glasgow, *Data Brokers: Should They Be Reviled or Revered?*, *in* Cambridge Handbook of Consumer Privacy 25 (Evan Selinger, Jules Polonetsky & Omer Tene eds., 2018) (canvassing the apparent benefits that brokers bring to the economy, innovation, and consumers).

[12] Thomas E. Kadri, *Platforms as Blackacres*, 68 UCLA L. Rev. 1184, 1184–87 (2022) (discussing how researchers use data to "understand the effects of digital technologies, to oversee the influence that platforms wield, and to hold accountable the private actors that curate our experiences on the internet"); Thomas E. Kadri, *Digital Gatekeepers*, 99 Tex. L. Rev. 951, 977–82 (2021) (detailing how researchers rely on data to provide critical insights to the public).

[13] *See generally* Eugene Volokh, *Cheap Speech and What It Will Do*, 104 Yale L.J. 1805 (1995) (predicting that new technologies enabled by the internet will alter information flows by making speech "cheap").

Another set of purported benefits relate to consumers, largely stemming from how businesses use brokered data. In particular, human information fuels the datasets and algorithms that help companies target ads and develop products. The resulting corporate revenue could, at least theoretically, yield cheaper or better services for consumers. I'm skeptical that this species of informational capitalism is in the public's interest,[14] but debunking this defense of data brokerage is not essential. Even if the commercial benefits are substantial, we should not scoff at the serious harms tied to the broker industry.

Though there are many harmful facets of data brokerage, I'll focus here on only one: how brokers enable and exacerbate interpersonal abuse. Most directly, brokers' dossiers can be treasure troves for abusers, who can plunder them for information with just a few clicks and bucks. In Amy Boyer's case, Youens paid a broker $45 for her Social Security number, $30 for her home address, and $109 for her work address.[15] These sums might already seem trifling given the vile result, but many brokers offer much more for far less. In 2013, for instance, a stalker bought Judge Timothy Corrigan's home address for less than $2 and later shot bullets at his house, missing the judge's head by a mere 1.6 inches.[16]

These jarring anecdotes tell part of the story of how brokers enable and exacerbate abuse, but the phenomenon needs more interrogation to show its full scope. To do so, we must unpack how the law can be ineffective and even injurious when responding to brokered abuse.

10.3 THE LAW'S ROLE IN BROKERED ABUSE

There are at least four common regulatory responses to brokered abuse: prohibiting abusive acts, mandating broker transparency, limiting data collection, and restricting data disclosure. Though each measure has some merit, none will suffice. Worse still, recent privacy laws can even inadvertently inflict psychological harms on people seeking to recover from abuse. Let us explore how.

10.3.1 *Prohibiting Abusive Acts*

Regulating abusive acts offers a path to reducing brokered abuse. If we target the underlying abuse, the thought goes, we needn't regulate data brokerage. While this

[14] *See generally* Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (2019) (exploring how informational-capitalist discourses have entrenched corporate power); Ari Ezra Waldman, Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power (2021) (critiquing the corporate-friendly privacy discourses that shape the legal and technical work sustaining informational capitalism).

[15] Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1005–06 (N.H. 2003). Police also unearthed Youens's plan to find and murder Boyer's family, though he committed suicide before carrying it out. *The Amy Boyer Case*, Elec. Privacy Info. Ctr. (June 15, 2006), https://perma.cc/G6J7-Z8TF.

[16] Hannah Elias Sbaity, *Private Lives at Home and Public Lives in Court: Protecting the Privacy of Federal Judges' Home Addresses*, 28 J. Intell. Prop. L. 475, 485–86 (2021).

approach is attractive in theory and even viable in certain cases, it's deficient for several reasons.

A host of laws directly regulate abuse, including criminal and tort liability for stalking, harassment, physical violence, doxing, privacy invasions, and voyeurism.[17] But even if these anti-abuse laws retroactively punish harmful acts or vindicate victims' interests in some cases, the continued prevalence of abuse suggests that any prospective deterrence caused by the threat of liability is inadequate. Even when abuse is deterred, these laws do little to lessen people's anxiety when their information is circulating online because they might lack confidence that any deterrence will hold.

To make matters worse, some anti-abuse laws can inadvertently increase people's risks of abuse. For example, when liability depends on an entity intending or knowing that their actions will cause harm, brokers have an incentive to remain ignorant about how brokered data is being used. Consider California's approach to protecting stalking victims who register with the state. A special anti-doxing law prohibits anyone, including brokers, from posting a registered victim's home address, phone number, or image on the internet with the "intent" to "[t]hreaten" the victim or "[i]ncite" a third person to cause "imminent" bodily harm "where the third person is likely to commit this harm."[18] With all these caveats, brokers can comfortably dodge liability by sharing data without asking questions.[19] Indeed, the standard data-brokerage business model – which relies on mass and indiscriminate data disclosures to anyone willing to pay – is incompatible with these kinds of scienter requirements because they implausibly suggest that brokers engage in case-specific deliberation or investigation before sharing data. And yet removing these caveats might pose a different problem because a law that broadly penalizes disclosing information might be vulnerable to constitutional challenges under the First Amendment.[20]

[17] *See, e.g.*, Ga. Stat. Ann. § 16–5-90 (criminalizing the offense of "stalking" when a person "follows, places under surveillance, or contacts another person at or about a place or places without the consent of the other person for the purpose of harassing and intimidating the other person"); Cal. Pen. Code § 653.2 (criminalizing the nonconsensual "electronic distribut[ion]" of "personal identifying information" with "intent to place another person in reasonable fear for his or her safety" and "for the purpose of imminently causing that other person unwanted physical contact, injury, or harassment, by a third party"); *see also* Eugene Volokh, *One-to-One Speech vs. One-to-Many Speech, Criminal Harassment Laws, and "Cyberstalking"*, 107 Nw. U. L. Rev. 731 (2013) (exploring the scope and constitutionality of stalking and harassment laws).

[18] Cal. Gov. Code § 6208.1.

[19] Similar challenges arise in holding brokers vicariously liable for helping abusers. Liability for conspiracy or aiding and abetting requires substantial assistance, encouragement, or even a common plan to commit an illegal act. Inadvertently or not, these doctrines reward brokers' willful blindness when a person has dangerous designs with brokered data.

[20] *See* Kadri, *Platforms as Blackacres*, *supra* note 12, at 1234–40. There's no doubt that First Amendment arguments advanced by brokers could chill or weaken regulatory efforts in this space, in part because companies can plausibly argue that doctrine developed in different

Beyond substance, think practicalities. Anti-abuse laws often require a victim's prolonged and active participation in pressing charges or filing lawsuits. There's good reason to empower and involve victims in these legal processes, but the processes themselves can impose burdens that many victims are unable or unwilling to bear. Interacting with police, prosecutors, lawyers, and judges might dissuade some people, while some might also struggle practically or financially to bring civil claims – realities that disproportionately affect those who are already marginalized. Even setting aside these burdens, many people will fret about initiating matters of public record that could further jeopardize their obscurity and safety.[21]

Finally, anti-abuse laws usually will not offer the obscurity remedies that some people will seek. Even if they do (or if such a remedy is eventually negotiated through settlement), legal proceedings move too slowly to address the exigent and immediate dangers that people face. To cap it all off, different brokers are constantly adding to their data stockpiles, so people would need to file new claims against new parties every time new information pops up online.

In short, laws prohibiting abusive acts fail to disturb essential features of brokered abuse. Some regulations might even aggravate matters by encouraging brokers to maintain ignorance when dishing out data, while other legal processes can be too burdensome, risky, or ineffective to be worth a victim's while.

10.3.2 *Mandating Broker Transparency*

Another regulatory tool involves shedding light on data brokerage. While transparency laws can be helpful, they are ultimately insufficient. These laws come in different shapes and sizes, but we can distinguish two types based on their principal goals: administrative transparency that informs regulators and popular transparency that informs individuals. Each has value, but neither meaningfully abates brokered abuse.

Administrative transparency follows a two-step system to educate regulators about the broker industry. Brokers first register with a state agency to create a list of brokers doing business in the jurisdiction, then brokers disclose details about their practices (such as where they obtain data and how they handle complaints). Vermont and

media environments protects their use of information from public records. *See id.* (delving into precedent that limits the government's ability to restrict data flows once information enters the public sphere); *cf.* Cohen, *supra* note 14 (exploring how technology companies have been shielded from legal accountability). This chapter dodges many of these First Amendment questions, leaving them for fuller treatment in the future.

[21] *See* Thomas E. Kadri, Tort Law: Cases & Critique 77–78 (2d ed. 2022) (discussing how this so-called "Streisand Effect" can also be "a *legal* phenomenon" because "suing can garner greater attention, thereby worsening the privacy invasion sought to be remedied by the lawsuit").

California have such laws, and similar themes animate the Data Broker List Act introduced in Congress in 2021.[22]

Popular transparency, by contrast, mainly informs individuals. California, for instance, has passed "right to know" laws that force brokers to reveal details they'd rather conceal: what data they have and whether they have shared it.[23] Similar laws might even oblige brokers to grant people no-cost access to data about themselves, rather than forcing them to pay a fee.

Administrative transparency can help regulators grasp the broker industry and inform future legislation, while popular transparency can help motivated people learn something new about their exposure with particular brokers. But neither approach helps a person facing urgent threats from their information appearing online. There's also no guarantee that transparency will motivate further regulation; if anything, these milquetoast measures might sap political will from stronger proposals.[24] At best, then, transparency laws fiddle with some incentives underlying data brokerage. (Maybe brokers will disclose less data if they have to disclose how they are disclosing data?) At worst, these laws let brokers hide their harmful practices in plain sight while boasting about their regulatory compliance.

10.3.3 *Limiting Data Collection*

A third response to brokered abuse involves curtailing data collection. Again, there are promises and pitfalls to this approach. Laws of this ilk form a privacy mosaic for our information, but there are too many missing pieces to make a pleasing mural.

Longstanding regulations forbid obtaining data through deception, other laws bar intrusive surveillance like hacking, and various legal regimes give companies "gatekeeper rights" to deter data scraping from their websites.[25] These restrictions reach

[22] *See* Cal. Civ. Code §§ 1798.99.80 *et seq.*; 9 Vt. Stat. Ann. § 2430; S. 2290, 117th Cong., 1st Sess. (2021), https://perma.cc/C4Z4-QSQF. This approach has also been endorsed by the Federal Trade Commission and forty state attorneys general. *See* Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability (May 2014); Nat'l Ass'n of Attorneys General, *Federal Trade Commission Hearings on Competition and Consumer: Protection in the 21st Century: Public Comments of 43 State Attorneys General* (June 11, 2019), https://perma.cc/U7LD-TF6A. *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 747 (2017) (exploring how state attorneys general have been "laboratories of privacy enforcement" and "expanded the frontiers of privacy law").

[23] Cal. Civ. Code § 1798.115.

[24] *See* Pozen, *supra* note 9, at 135–41 (exploring how soft-touch and targeted transparency mandates in consumer-protection law have "evolved into a stock substitute for more robust and direct regulation"); *cf. id.* at 134 (arguing that reliance on transparency mandates in campaign-finance reform helped to thwart restrictions on election spending).

[25] *See, e.g.*, Kadri, *Digital Gatekeepers*, *supra* note 12, at 957–69 (discussing how cyber-trespass laws empower companies to act as "gatekeepers" on their websites); Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003) (endorsing privacy and negligence tort claims if a broker obtains information through deceptive means); 18 U.S.C. § 1039 (making it a federal crime to

only a subset of brokers' activities because gobs of data can be gathered without running afoul of any law.[26] Most importantly, many of these laws do not apply when brokers get data from public records or other publicly accessible sources.[27]

More recently, a new vintage of data-privacy laws has unsettled the broker industry by prohibiting the nonconsensual collection of people's information. But even these stricter rules often contain caveats that let brokers thrive. The California Consumer Privacy Act, for example, provides that the types of "personal information" protected by the law do not include "publicly available information or lawfully obtained, truthful information that is a matter of public concern" – an exception that covers vast troves of brokered data and endorses many broker practices that leave abuse victims vulnerable.[28]

In light of these carveouts for publicly accessible information, one approach to limiting data collection focuses on the state's role in furnishing brokered data.[29] Brokers sustain their services with information from public records like property

fraudulently obtain "confidential phone records information"); 18 U.S.C. § 2511 (making it a federal crime under the Wiretap Act to "intentionally intercept[] … any wire, oral, or electronic communication"); 18 U.S.C. § 1030(a)(2)(C) (making it a federal crime under the Computer Fraud and Abuse Act to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] … information from any protected computer"). Whether brokers are liable for scraping and other types of cyber-trespass is a complex matter (and mixture) of criminal, tort, and contract law, but suffice to say that brokers can still collect ample data and steer well clear of these restrictions. *See, e.g.*, Kadri, *Digital Gatekeepers*, *supra* note 12 (discussing liability for scraping under the Computer Fraud and Abuse Act and other cyber-trespass laws); Kadri, *Platforms as Blackacres*, *supra* note 12 (discussing the First Amendment implications of laws regulating scraping).

[26] *See generally* Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213 (2018) (exploring how law shapes and enables extractive practices of appropriating personal information).

[27] *See, e.g.*, 18 U.S.C. § 2511(2)(g)(i) (providing that "[i]t shall not be unlawful" under the Stored Communications Act, 18 U.S.C. § 2701, to "access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public"); hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1201 (9th Cir. 2022) (holding that the Computer Fraud and Abuse Act, § 1030(a)(2)(C), likely does not apply "when a computer network generally permits public access to its data"); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 471, 473–74, 495–96 (1975) (outlining First Amendment limits on privacy tort claims based on accessing information already in the public domain); Kadri, *Platforms as Blackacres*, *supra* note 12, at 1234–40 (analyzing constitutional doctrine in this area).

[28] *See* CAL. CIV. CODE § 1798.140; *see also* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 106, 116–17 (2020) (discussing how brokers are regulated by the European Union's General Data Protection Regulation).

[29] Though this chapter cannot flesh out this point, it's high time to reconsider the state's complicity in supplying brokered data. *See generally* Daniel J. Solove, *Access and Aggregation: Privacy, Public Records, and the Constitution*, 86 MINN. L. REV. 1137 (2002) (urging a rethinking of the regulation of public records in light of new technologies in the Information Age); Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1818–24 (2021) (advocating for limits on collecting intimate information to protect sexual privacy); Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459, 459 (2019) (critiquing how "labeling information as public often functions as a permission slip for

deeds, voter rolls, and marriage licenses. To partially stem this flow, most states have confidentiality programs to allow abuse victims to conceal certain information from state documents.[30] On the plus side, these measures are unlikely to raise First Amendment red flags because nothing forces the government to collect (or publish) the kind of identifying information that most likely endangers people's obscurity.[31] But while limiting government data collection (and publication) brings significant benefits, even the broadest restrictions are insufficient. Public records, after all, are but one source of human information. Most importantly, brokers can still buy data from other companies and gather it from other public websites. Tinkering with public records turns off the cold tap but leaves the hot water flowing.

10.3.4 *Restricting Data Disclosure*

A final way to tackle brokered abuse involves controlling data disclosure. This approach conceivably offers great potential for people seeking to stop brokers publicizing their information online. But the devil is in the details. Many disclosure regulations either do little to thwart abuse or even harm people trying to protect themselves.

Some disclosure rules aren't aimed specifically at either data or brokers, such as tort liability for publicly disclosing certain sensitive information,[32] while other recent

surveillance and personal data practices"); Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 Harv. J.L. & Tech. 111 (2017) (investigating people's privacy interests in public records through an empirical study). The flip side of this symbiotic relationship is also true: we should also reconsider brokers' roles in furnishing the state with data. *See, e.g.*, Cmty. Just. Exch., From Data Criminalization to Prison Abolition (2022), https://perma.cc/DQV2-9SS3 (critiquing "data criminalization": "the creation, archiving, theft, resale and analysis of datasets that mark certain people as threats and risks, based on data culled about them from state and commercial sources").

[30] *Address Confidentiality Program*, N.Y. State, https://perma.cc/V6AK-3MWM (outlining how victims may shield their addresses in some state records by creating a substitute address); *About Safe at Home*, Cal. Sec'y State, https://perma.cc/4AVJ-TDK3 (detailing how victims may seek confidential name changes and voter registration); *see also* Davis Wright, Address Confidentiality Programs: Resource Guide (2022) (surveying all fifty states and noting that only Alaska, South Carolina, South Dakota, Utah, and Wyoming lack any form of address-confidentiality program for abuse victims).

[31] *See* Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 Wm. & Mary L. Rev. 1501 (2015) (arguing that most laws regulating the collection, use, and disclosure of personal data should survive First Amendment challenges). Though I cover *collection* and *disclosure* here, I omit discussion of *use* restrictions because, at least in the United States, they have offered less promise to restrain brokered abuse. One law frequently touted as relevant to brokers is the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 k, which prohibits employers from using certain data in hiring decisions. Brokers enter the picture because FCRA arguably restricts them from knowingly providing employee-screening data. Even if this contentious interpretation were accepted, such a narrow and consumer-focused law does little to address interpersonal abuse.

[32] *See* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Calif. L. Rev. 957, 978–1008 (1989) (dissecting the privacy tort of public disclosure of private facts).

proposals would make brokers pay for selling people's data or ban them from sharing location and health information. Such constraints meddle with brokerage around the margins, but none brings fundamental reform and some plausibly exempt publicly accessible data.[33]

Given these limitations, let us focus instead on modern laws providing rights to conceal or remove information from broker databases or websites. California offers a rare example in the United States of providing these legally mandated obscurity rights, so we'll use it as a short case study to examine the virtues and vices of such a regulatory regime. Under the state's general "right to opt-out," all Californian consumers may direct businesses not to sell their personal information to third parties, meaning that the company must not disclose their data for profit once a person exercises their obscurity right.[34] But California law also goes one step further. Abuse victims who register with the state's Safe at Home program have more expansive obscurity rights. Of particular note, brokers cannot knowingly display a victim's phone number or home address on the internet. If a victim asserts their reasonable fear related to that information, a broker must conceal the data for four years and could face injunctions, court costs, and attorney's fees for noncompliance. And if anyone, including a broker, displays or sells the information with intent to cause certain harms, victims may seek treble damages and receive a $4,000 fine per violation. To help implement the law's protections, California provides an online opt-out form that victims can use to invoke their obscurity rights.[35]

Though California's goals are laudable, this innovative approach fails to grapple with the realities of abuse. Under these laws, Californians must engage in extensive "privacy self-management" because the state forces them to exercise obscurity rights on a company-by-company basis.[36] Even the Safe at Home opt-out process – which was presumably designed with abuse victims in mind – operates from this fragmented premise by requiring victims to approach brokers individually and submit

[33] *See* Own Your Own Data Act, S. 806, 116th Cong., 1st Sess. (2019) (providing that "[e]ach individual owns and has an exclusive property right in the data that an individual generates on the internet"); Ignacio Cofone, *Beyond Data Ownership*, 43 Cardozo L. Rev. 501 (2021) (exposing flaws in the property approach to personal information); Health and Location Data Protection Act, S. 4408, 117th Cong., 2d Sess. (2022) (prohibiting brokers from sharing location and health data unless such data constitutes "newsworthy information of legitimate public concern").

[34] Cal. Civ. Code § 1798.120.

[35] Cal. Gov. Code § 6208.1; *Program Services*, Cal. Sec'y State, https://perma.cc/DER2-3Q86.

[36] For background on privacy-self management, *see* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1882–83 (2013), and Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 Stan. Tech. L. Rev. 431, 444 (2016). Technological tools like the Global Privacy Control are seeking to streamline this process by enabling people to automatically assert their obscurity rights through settings on their browsers. Though this initiative still creates self-management burdens that will likely dampen its efficacy, it could be a step in the right direction. *See* Glob. Priv. Control, https://perma.cc/QE8C-4972.

forms to each one regularly. Brokers, after all, continuously replenish their stocks, and concealing *some* data does not stop *other* data from soon taking its place. Given these features of the broker industry, laws like California's could actually entrench a disaggregated and detrimental obscurity process because brokers can seize on their legal compliance to justify not offering better services.

10.4 THE HARMS OF BROKERED ABUSE

With this legal survey in mind, let us return to the matter of harms: How do brokers enable and exacerbate abuse? How is the law inadequate and complicit? And how might legal procedures even contribute toward a person's suffering?

To answer these questions, I return to obscurity – a notion of privacy concerned with "the difficulty and probability of discovering or understanding information."[37] As Woodrow Hartzog and Evan Selinger have observed, obscurity can be a "protective state" that serves valuable privacy-dependent goals like "autonomy, self-fulfillment, socialization, and relative freedom from the abuse of power."[38] Understanding the full scope of brokered abuse requires parsing how data brokerage, including its surrounding legal constructs, undermines obscurity. As we'll see, brokered abuse encompasses an array of *intrinsic* and *extrinsic* harms, all of which implicate a person's obscurity.

10.4.1 *Intrinsic Harms*

Abuse. As an initial matter, brokers routinely create privacy losses by sharing people's information. Though this core of brokerage is not intrinsically harmful, such privacy *losses* can engender privacy *harms*.[39] Some of these privacy harms, to use Ignacio Cofone's terminology, are "consequential" because they are "external to privacy interests but occur as a consequence of privacy violations."[40] Brokers facilitate the surveillance of victims and their kin by systematically sharing personal information. An abuser armed with brokered data can perpetrate a slew of

[37] Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1355 (2015).

[38] Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way to Think About Your Data than "Privacy"*, ATLANTIC (Jan. 17, 2013), https://perma.cc/38TV-8KTL.

[39] *See* Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1042, 1049–55 (2018) (connecting but distinguishing the ideas of "privacy loss" and "privacy harm"); Ignacio Cofone, *Privacy Standing*, 2022 U. ILL. L. REV. 1367 (further developing these concepts in the context of standing to bring privacy claims); *see also* Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1131, 1143 (2011) (arguing that subjective and objective privacy harms represent "the anticipation and consequence of a loss of control over personal information"); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 830–61 (2022) (offering a typology of privacy harms to show privacy's instrumental value in seven different contexts).

[40] *See* Cofone, *supra* note 39, at 1398, 1403–05.

"consequential" physical, emotional, economic, and reputational harms. This might not be a broker's goal, but it's certainly their role.

Risk. Beyond the direct harm of actually enabling abuse, brokers commit the kindred harm of increasing the risk of abuse by making it easier to surveil a person and their family, friends, or associates. This risk, in turn, can cause anxiety even if no abusive act ever occurs.[41] Without regulatory intervention, these threats will only grow as data proliferates and new technologies, like facial-recognition surveillance, further wreck obscurity.[42]

Isolation. Brokers also rob people of agency to "control their visibility within public space."[43] As Scott Skinner-Thompson has argued, digital and physical surveillance can cause forced publicity, which might then deter people from participating in public life.[44] This cycle, unsurprisingly, has unequal repercussions for those who are socially marginalized already – a special concern here because victims often hail from marginalized groups and because abuse can have ostracizing effects regardless of one's preexisting social status and personal characteristics.[45] Data brokerage can intensify a victim's isolation by foisting visibility on them, creating yet more reasons for them to retreat entirely from public spaces.

10.4.2 *Extrinsic Harms*

Some people respond to this trio of intrinsic harms – abuse, anxiety, and isolation – by trying to cull information from broker databases. Easier said than done. As we have seen, people must beg brokers to conceal their data with little guarantee of success, especially in jurisdictions where legal remedies are absent or incomplete. At best, people in places like California can contact every single broker separately to

[41] *Cf.* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 Tex. L. Rev. 737 (2018) (arguing that risk and anxiety can be legally cognizable harms caused by data breaches).

[42] *See* Amanda Levendowski, *Resisting Face Surveillance with Copyright Law*, 100 N.C. L. Rev. 1015, 1018, 1022–35 (2022) (identifying injustices of "face surveillance" – a term that "embraces multiple biometric systems that use algorithms to analyze faces, such as face detection, face classification, and . . . face recognition"); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461, 1485 (2019) (discussing the threats posed by facial-recognition technology); Woodrow Hartzog & Evan Selinger, *Why You Can No Longer Get Lost in the Crowd*, N.Y. Times (Apr. 17, 2019), https://perma.cc/C2ST-9UUJ (exploring the importance of obscurity and observing that "[t]hreats to our obscurity are growing" due to advances in technology).

[43] Scott Skinner-Thompson, *Agonistic Privacy & Equitable Democracy*, 131 Yale L.J. F. 454, 456 (2021).

[44] *Id.* at 454–56, 459–61.

[45] *See* Mary Anne Franks & Ari Ezra Waldman, *Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions*, 78 Md. L. Rev. 892, 896 (2019); Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 Law & Soc. Inquiry 987, 1009 (2019); Thomas E. Kadri, *Drawing Trump Naked: Curbing the Right of Publicity to Protect Public Discourse*, 78 Md. L. Rev. 899, 950–51 (2019).

exercise their legal rights. The result? People facing physical and psychological peril must approach each broker individually over and over again. At a time of high vulnerability, this obscurity process creates a pair of extrinsic harms that are partly constructed by legal rules and procedures.

Annoyance. The first harm can be styled as annoyance, though it covers a range of unwanted emotions. Some people might reasonably feel indignant about having to demand their obscurity. (Imagine someone complaining: "It's *my* data, not *theirs*, so *they* should have to ask *me* before using it! Why should *I* have to contact *them*?") Others might resent spending time filling out forms or navigating brokers' laborious and complex bureaucracies. Some people might feel exasperated at how futile it all seems, especially given that "grey holes" in privacy law might give brokers enough room to resist obscurity requests or refill their databases.[46] Absent some compelling justification, the law should not be complicit in cultivating negative reactions to exercising legal rights. Feeling indignant, resentful, or exasperated is both unpleasant and likely to dissuade people from enforcing their rights.

Trauma. Taking annoyance seriously is important to understanding the law's failure to address brokered abuse. But to culminate this chapter, I want to stress something different and underappreciated. For abuse victims, an arduous and dispersed obscurity process can inflict a harm that goes beyond mere hassle or frustration. It's more than a matter of transaction costs. It's more even than a question of abuse and anxiety. Instead, it's about trauma – and how the law's failure to consider the role of trauma represents a failure of empathy toward victims of abuse.

The basic point is this: The process of preventing brokers from sharing information can trigger psychological harm by forcing victims to repeatedly revisit their abuse and recognize their vulnerability. A disaggregated and inefficient obscurity process might irritate some people, but the burden it can impose on victims is likely distinct and severe. In short, the obscurity process itself can be traumatic.

"Trauma is the experience and resulting aftermath of an extremely distressing event or series of events, such as disaster, violence, abuse, or other emotionally harmful experiences."[47] Though further research is required to explore how trauma manifests in the context of brokered abuse, existing studies point to likely connections between abuse, trauma, and technology. For example, a recent interdisciplinary study by researchers working directly with victims in the Clinic to End Tech Abuse at Cornell University examines how people's interactions with digital

[46] *Cf.* Alicia G. Solow-Niederman, *Algorithmic Grey Holes*, 5 J.L. & Innov. 116 (2023) (exploring the idea of how "grey holes" in law can include procedures that create the appearance but not the reality of constraints on government action).

[47] *See* Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart & Nicola Dell, *Trauma-Informed Computing: Towards Safer Technology Experiences for All*, CHI'22: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems 1 (2022).

https://doi.org/10.1017/9781009174411.013 Published online by Cambridge University Press

technologies can cause trauma in the context of interpersonal abuse. As the authors observe based on a series of actual case studies, people's experiences with technology can "trigger existing trauma and even retraumatize a person," such as "when something in one's environment causes them to recall a traumatic experience, often with a recurrence of the emotional state during the original event."[48] Based on my own experiences – personally as an abuse victim and professionally when speaking with other victims – this accurately describes how prevailing obscurity processes involving data brokers can trigger trauma.

Even the most expansive obscurity rights fail to grapple with this extrinsic harm. Indeed, these laws risk aggravating matters by enshrining a decentralized process into law. While current procedures might be annoying for someone who's never faced abuse, for victims seeking obscurity it creates an extra injury that might further discourage them from enforcing their legal rights. Legislators have failed to account for the dynamics of interpersonal abuse from a victim's perspective. The law, it might be said, lacks empathy.

To compound matters, current processes to regain obscurity are often ineffective. Brokers can simply shun removal requests in the forty-odd states that lack data-privacy laws, and even a responsive broker can do no more than purge information from its own database. An abuser needs only one willing broker to facilitate surveillance, and the scattering of digital breadcrumbs among brokers can distress people even if an abuser never actually gets any data. A flawed obscurity process, then, solidifies all three intrinsic harms by enabling abuse, creating anxiety, and causing isolation, while also maintaining extrinsic harms like annoyance and trauma.[49]

I leave the matter of addressing brokered abuse for another day, but one thing seems clear: There's a dire need for an effective and empathetic obscurity process.[50] Though it's impossible to say how many people are harmed through brokered data, we know that many forms of technology-enabled abuse are rampant, rising, and ruinous. Recent empirical research has shown how abusers are exploiting technologies to intimidate, threaten, monitor, impersonate, and harass.[51] This essential work substantiates earlier scholarship revealing how technology can facilitate interpersonal harms and deepen social inequities.[52] We know, too, that abuse victims suffer

[48] *Id.* at 4–6.

[49] *See* Kadri, *supra* note 6, at 1095–96 (discussing how the mere existence of technologies that enable stalking can instill paranoia in abuse victims); Mara Hvistendahl, *I Tried to Get My Name Off People-Search Sites. It Was Nearly Impossible*, Consumer Reps. (Aug. 20, 2020), https://perma.cc/T52R-LG34.

[50] *See* Kadri, *supra* note 6, at 1078–80, 1118–19 (arguing that empathy should be a guiding regulatory principle in this area).

[51] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart & Nicola Dell, *"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology*, Ass'n Computing Mach. (2018).

[52] *See, e.g.*, Danielle Citron, Hate Crimes in Cyberspace (2014); Ari Ezra Waldman, *Safe Social Spaces*, 96 Wash. U. L. Rev. 1535 (2019); Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 Colum. J. Gender & L. 224 (2011).

significantly higher rates of depression, anxiety, insomnia, and social dysfunction than the general population.[53] Given these realities, we should not turn a blind eye to brokered abuse.

10.5 CONCLUSION

Data brokers are abuse enablers. By sharing people's information, brokers thwart obscurity, stimulate surveillance, and ultimately enable interpersonal abuse. This chapter has canvassed four regulatory responses to brokered abuse. Though these existing measures have some merit, none is adequate, and some laws can even make matters worse. Put simply, the current legal landscape is neither effective nor empathetic.

Of particular and yet underappreciated concern, the prevailing broker-by-broker approach to regaining obscurity likely causes victims' trauma by forcing them to engage repeatedly with their abuse and vulnerability. The flaws of this obscurity process also leave people vulnerable to serious physical, psychological, financial, and reputational harms. Regulating brokered abuse should be a priority for both lawmakers and technologists.

[53] Eric Blaauw, Frans W. Winkel, Ella Arensman, Lorraine Sheridan & Adriënne Freeve, *The Toll of Stalking: The Relationship between Features of Stalking and Psychopathology of Victims*, 17 J. Interpersonal Violence 50, 57–58 (2002); *see also* Ari Ezra Waldman, *Amplifying Abuse: The Fusion of Cyberharassment and Discrimination*, 95 B.U. L. Rev. Annex 83, 83 (2015) (discussing how cyberharassment victims commonly experience anxiety, panic attacks, fear, post-traumatic stress disorder, anorexia, bulimia, and clinical depression).